

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年10月18日 (18.10.2001)

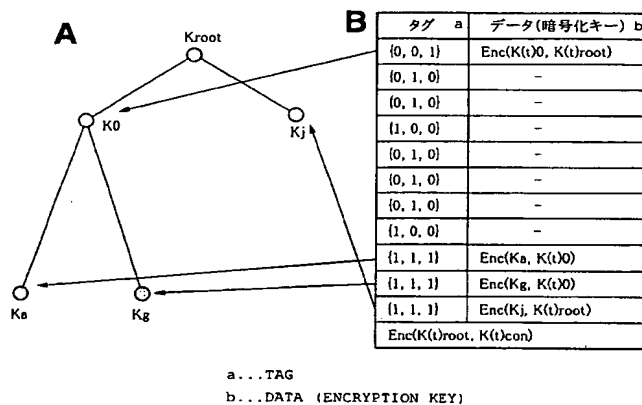
PCT

(10) 国際公開番号
WO 01/78299 A1

- (51) 国際特許分類: H04L 9/00, G06F 17/60, G11B 20/10, 20/12 [JP/JP]. 大石丈於 (OISHI, Tateo) [JP/JP]. 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/02929
- (22) 国際出願日: 2001年4月4日 (04.04.2001) (74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (81) 指定国 (国内): CA, CN, IN, KR, RU, SG, US.
- (30) 優先権データ: (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 特願2000-105329 2000年4月6日 (06.04.2000) JP
特願2000-179692 2000年6月15日 (15.06.2000) JP
特願2000-317803 2000年10月18日 (18.10.2000) JP
- 添付公開書類:
— 国際調査報告書
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo)

(54) Title: INFORMATION PROCESSING SYSTEM AND METHOD

(54) 発明の名称: 情報処理システム及び方法



(57) Abstract: An effective key block (EKB) used for key distribution structure of tree structure is re-structured to a simplified two-branch or multi-branch tree in which a decodable end node or leaf is at the lowest layer so as to create a re-structured layered tree according to only a key corresponding to the node or leaf of the re-structured layered tree. A tag as identification data about the tree position of an encryption key stored in the EKB is stored. In the tag, not only the position identification but data for judging if encryption key data is present in the EKB is stored. The amount of data in the EKB is greatly reduced and the decoding by a device is simplified. Thus, providing an information processing system and method enabling reduction of the amount of data in an Effective key block (EKB) used for an encryption key structure of tree structure.

[続葉有]

BEST AVAILABLE COPY

WO 01/78299 A1



(57) 要約:

ツリー構造のキー配布構成に用いる有効化キーブロック（E K B）を、復号可能な末端ノード又はリーフを最下段として簡略化した2分岐または多分岐型ツリーを再構築して、再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて生成する。さらに、E K Bに格納した暗号化キーのツリー位置の識別データとしてのタグを格納する。タグは、位置識別のみならず、E K B内の暗号化キーデータの有無を判別するデータを格納した構成とした。E K Bの大幅なデータ量削減が実現するとともに、デバイスでの復号処理も簡易化される。すなわち、ツリー構造の暗号化キー構成に用いる有効化キーブロック（E K B）のデータ量の削減を可能とした情報処理システム及び方法を実現する。

明細書

情報処理システム及び方法

技術分野

本発明は、情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステム及び方法に関する。特に、木構造の階層的鍵配信方式を用い、さらに、階層的鍵配信ツリーを配信デバイスに応じて再構築して配信キープロックに含まれるデータ量を削減することにより、配信メッセージ量を小さく抑えて、コンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とする情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはDVD、CD等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはPC等に付属する記録再生機器内の記録デバイス、例えばメモリカード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

ビデオゲーム機器、PC等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはDVD、CD等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データの

メモリ領域として使用されるRAM、ROM等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。したがって、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパ

スワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行う。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはR S A (Rivest-Shamir-Adleman) 暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはDVD、CD等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行う。一般的な認証処理においては、相手の確認を行うとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデー

タ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行う。認証方式には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通な鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

発明の開示

本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とするとともに、階層的鍵配信ツリーを配信デバイスに応じて再構築して配信キーブロックに含まれるデータ量を削減することにより、暗号化キーのデータ量を削減し、データ送信の負荷を軽減するとともに、各デバイスにおける暗号化キー取得のための処理の軽減を可能とした情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

本発明に係る情報処理システムは、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムである。個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される暗号化メッセージデータについての復号処理をキーセットを使用して実行する暗号処理手段を有する。デバイスに提供される暗号化メッセージデータは、階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含む有効化キーブロック（EKB）の復号処理によって得られる更新ノードキーによって暗号化されたデータ構成である。有効化キーブロック（EKB）は、暗号化キーデータによって構成されるデータ部と、デー

タ部に格納される暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む構成である。

さらに、本発明の情報処理システムの一実施態様において、有効化キーブロック (EKB) に含まれる暗号化キーデータは、階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化したデータである。タグ部に格納される位置識別データは、有効化キーブロック (EKB) に格納された 1 以上の暗号化キーデータ各々のノード位置の下位の左右ノード又はリーフ位置の暗号化キーデータの有無を示すタグとして構成されている。

さらに、本発明の情報処理システムの一実施態様において、有効化キーブロック (EKB) に含まれる暗号化キーデータは、有効化キーブロック (EKB) を復号可能な末端ノード又はリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成されている。タグ部に格納される位置識別データは、有効化キーブロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成である。

さらに、本発明の情報処理システムの一実施態様において、有効化キーブロック (EKB) に含まれる暗号化キーデータは、有効化キーブロック (EKB) を復号可能な末端ノード又はリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成されている。タグ部に格納される位置識別データは、有効化キーブロック (EKB) に格納された 1 以上の暗号化キーデータ各々のノード位置の下位の左右ノード又はリーフ位置の暗号化キーデータの有無を示すタグと、タグに対応する暗号化キーの格納の有無を示すデータを含む。

さらに、本発明の情報処理システムの一実施態様において、再構築階層ツリーは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して構成されるツリーである。

さらに、本発明の情報処理システムの一実施態様において、有効化キーブロック (EKB) に含まれる暗号化キーデータは、有効化キーブロック (EKB) を

復号可能な末端ノード又はリーフを最下段とした簡略化した多分岐型ツリーにおいて、末端ノード又はリーフと、多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーの頂点ノード及び末端ノード又はリーフに対応するキーのみに基づいて構成されている。タグ部に格納される位置識別データは、有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを含む構成である。

さらに、本発明の情報処理システムの一実施態様において、再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノード又はリーフとを直接接続した3以上の分岐を持つツリーである。

さらに、本発明の情報処理システムの一実施態様において、デバイスにおける暗号処理手段は、有効化キーブロック（EKB）のタグ部のデータにより、暗号化キーデータを順次抽出して、復号処理を実行し、更新ノードキーを取得し、取得した更新ノードキーにより暗号化メッセージデータの復号を実行する構成である。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、プログラムコードである。

本発明に係る情報処理方法は、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理方法である。この情報処理方法は、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した

暗号化キーデータを含むデータ部と、データ部に格納される暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック (E K B) を生成する有効化キーブロック (E K B) 生成ステップと、更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップとを有する。

さらに、本発明の情報処理方法の一実施態様において、階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、暗号化メッセージデータについての復号処理をキーセットを使用して実行する復号処理ステップを有する。

さらに、本発明の情報処理方法の一実施態様において、有効化キーブロック (E K B) 生成ステップは、階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化して暗号化キーデータを生成するステップと、有効化キーブロック (E K B) に格納される 1 以上の暗号化キーデータ各々のノード位置の下位の左右位置のノード又はリーフ位置の暗号化キーデータの有無を示すタグを生成してタグ部に格納するステップとを含む。

さらに、本発明の情報処理方法の一実施態様において、有効化キーブロック (E K B) 生成ステップは、有効化キーブロック (E K B) を復号可能な末端ノード又はリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、再構築階層ツリーの構成ノード又はリーフに対応するキーのみに基づいて有効化キーブロック (E K B) を生成するステップと、有効化キーブロック (E K B) のタグに対応する暗号化キーの格納の有無を示すデータをタグ部に格納するステップとを含む。

さらに、本発明の情報処理方法の一実施態様において、再構築階層ツリーを生成するステップは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して実行されるツリー生成処理である。

さらに、本発明の情報処理方法の一実施態様において、有効化キーブロック (E K B) 生成ステップは、有効化キーブロック (E K B) を復号可能な末端ノ

ード又はリーフを最下段とした簡略化した多分岐型ツリーにおいて、末端ノード又はリーフと、多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーを生成するステップと、有効化キープブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータをタグ部に格納するステップとを含む。

さらに、本発明の情報処理方法の一実施態様において、再構築階層ツリーの生成ステップにおいて生成する再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノード又はリーフとを直接、接続した3以上の分岐を持つツリーとして生成する。

さらに、本発明の情報処理方法の一実施態様において、復号処理ステップは、有効化キープブロック（EKB）のタグ部に格納された位置識別データに基づいてデータ部に格納された暗号化キーデータを順次抽出して順次復号処理を実行することにより更新ノードキーを取得する更新ノードキー取得ステップと、更新ノードキーにより暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含む。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、プログラムコードである。

さらに、本発明に係る情報記録媒体は、データを格納した情報記録媒体である。この情報記録媒体は、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーに

よって暗号化した暗号化キーデータによって構成されるデータ部と、データ部に格納される暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（EKB）と、更新ノードキーによって暗号化したメッセージデータとを格納している。

さらに、本発明の情報記録媒体の一実施態様において、有効化キーブロック（EKB）に含まれる暗号化キーデータは、階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化したデータである。タグ部に格納される位置識別データは、有効化キーブロック（EKB）に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノード又はリーフ位置の暗号化キーデータの有無を示すタグとして構成されている。

さらに、本発明の情報記録媒体の一実施態様において、有効化キーブロック（EKB）に含まれる暗号化キーデータは、有効化キーブロック（EKB）を復号可能な末端ノード又はリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成されている。タグ部に格納される位置識別データは、有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを含む構成である。

本発明に係るプログラム提供媒体は、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）の生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体である。コンピュータ・プログラムは、有効化キーブロック（EKB）を復号可能な末端ノード又はリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、再構築階層ツリーの構成ノード又はリーフに対応するキーのみに基づいて有効化キーブロック（EKB）を生成するステップと、有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示す

データをタグ部に格納するステップとを含む。

本発明では、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、例えばコンテンツデータの暗号鍵であるコンテンツキー若しくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キーブロックとともに配信する構成としている。

さらに、有効化キーブロックを暗号化キーデータ部と、暗号化キーの位置を示すタグ部とによって構成し、データ量を少なくし、デバイスにおける復号処理を用意かつ迅速に実行することを可能としている。本構成により、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

なお、本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図1は、本発明の情報処理システムの構成例を説明する図である。

図2は、本発明の情報処理システムにおいて適用可能な記録再生装置の構成例

を示すブロック図である。

図 3 は、本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

図 4 A 及び図 4 B は、本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック (EKB) の例を示す図である。

図 5 は、本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック (EKB) を使用した配布例と復号処理例を示す図である。

図 6 は、本発明の情報処理システムにおける有効化キーブロック (EKB) のフォーマット例を示す図である。

図 7 A 乃至図 7 C は、本発明の情報処理システムにおける有効化キーブロック (EKB) のタグの構成を説明する図である。

図 8 A 及び図 8 B は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

図 9 は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

図 10 は、本発明の情報処理システムにおける有効化キーブロック (EKB) とコンテンツを記録媒体に格納した場合の対応について説明する図である。

図 11 A 及び図 11 B は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキーを送付する処理を従来の送付処理と比較した図である。

図 12 は、本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

図 13 は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 1) である。

図 14 は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (そ

の 2) である。

図 1 5 は、本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

図 1 6 は、本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キーブロック (E K B) と、コンテンツキーを併せて配信する処理を示す図である。

図 1 7 は、本発明の情報処理システムにおいて有効化キーブロック (E K B) と、暗号化プログラムデータを併せて配信する処理を示す図である。

図 1 8 は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値 (I C V) の生成に使用する M A C 値生成例を示す図である。

図 1 9 は、本発明の情報処理システムにおける有効化キーブロック (E K B) と、I C V 生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 1) である。

図 2 0 は、本発明の情報処理システムにおける有効化キーブロック (E K B) と、I C V 生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 2) である。

図 2 1 A 及び図 2 1 B は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値 (I C V) をメディアに格納した場合のコピー防止機能を説明する図である。

図 2 2 は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値 (I C V) をコンテンツ格納媒体と別に管理する構成を説明する図である。

図 2 3 は、本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

図 2 4 A 及び図 2 4 B は、本発明の情報処理システムにおける簡略化有効化キーブロック (E K B) の生成過程を説明する図である。

図 2 5 A 及び図 2 5 B は、本発明の情報処理システムにおける有効化キーブロック (E K B) の生成過程を説明する図である。

図 2 6 A 及び図 2 6 B は、本発明の情報処理システムにおける簡略化有効化キーブロック (E K B) (例 1) を説明する図である。

図 2 7 A 及び図 2 7 B は、本発明の情報処理システムにおける簡略化有効化キーブロック (E K B) (例 2) を説明する図である。

図 2 8 A 乃至図 2 8 C は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成について説明する図である。

図 2 9 A 乃至図 2 9 C は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成の詳細について説明する図である。

図 3 0 A 及び図 3 0 B は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成について説明する図である。

図 3 1 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのリザーブノードについて説明する図である。

図 3 2 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成での新規エンティティ登録処理シーケンスについて説明する図である。

図 3 3 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成での新規エンティティと上位エンティティの関係について説明する図である。

図 3 4 A 及び図 3 4 B は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成で用いるサブ E K B について説明する図である。

図 3 5 A 乃至図 3 5 D は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリボーク処理について説明する図である。

図 3 6 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリボーク処理シーケンスについて説明する図である。

図 3 7 A 及び図 3 7 B は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリボーク時の更新サブ E K B について説明する図である。

図 3 8 A 乃至図 3 8 D は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのエンティティリボーク処理について説明する図である。

図 3 9 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのエンティティリボーク処理シーケンスについて説明する図である。

図 4 0 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのリボークエンティティと上位エンティティの関係について説明する図である。

図 4 1 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのケイパビリティ設定について説明する図である。

図 4 2 は、本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのケイパビリティ設定について説明する図である。

図 4 3 A 及び図 4 3 B は、本発明の情報処理システムにおけるキー発行センタ（K D C）の管理するケイパビリティ管理テーブル構成を説明する図である。

図 4 4 は、本発明の情報処理システムにおけるキー発行センタ（K D C）の管理するケイパビリティ管理テーブルに基づく E K B 生成処理フロー図である。

図 4 5 は、本発明の情報処理システムにおける新規エンティティ登録時のケイパビリティ通知処理を説明する図である。

発明を実施するための最良の形態

[システム概要]

図 1 に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側 1 0 は、コンテンツ受信側 2 0 の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側 2 0 における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画像データ、音声データの再生、あるいは各種プログラムの実行等を行う。コンテンツの配信側 1 0 とコンテンツ受信側 2 0 との間のデータ交換は、インターネット等のネットワークを介して、あるいは D V D、C D 等の流通可能な記憶媒体を介して実行される。

コンテンツの配信側 1 0 は例えば所謂サーバとして構成され、ハードディスク

ドライブなどの情報記憶手段やCPUなどの情報処理装置を有する既存のパーソナルコンピュータで構成される。コンテンツの配信側10は後述するコンテンツプロバイダとして、あるいはサービスプロバイダやアプリケーションプロバイダが同等の機能を有していてもよい。コンテンツの配信側10のデータ配信手段としては、インターネット11、衛星放送12、電話回線13、DVD、CD等のメディア14等があり、一方、コンテンツ受信側20のデバイスとしては、パーソナルコンピュータ(PC)21、ポータブルデバイス(PD)22、携帯電話、PDA(Personal Digital Assistants)等の携帯機器23、DVD、CDプレーヤ等の記録再生器24、ゲーム端末等の再生専用器25等がある。これらコンテンツ受信側20の各デバイスは、コンテンツ配信側10から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア30から取得する。

[デバイス構成]

図2に、図1に示すコンテンツ受信側20のデバイスの一例として、記録再生装置100の構成ブロック図を示す。記録再生装置100は、入出力I/F(Interface)120、MPEG(Moving Picture Experts Group)コーデック130、A/D, D/Aコンバータ141を備えた入出力I/F(Interface)140、暗号処理手段150、ROM(Read Only Memory)160、CPU(Central Processing Unit)170、メモリ180、記録媒体195のドライブ190を有し、これらはバス110によって相互に接続されている。

入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D, D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D, D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとと

もに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ROM160は、記録再生装置によって処理されるプログラムデータを格納する。CPU170は、ROM160、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し（再生し）、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。

記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。ただし、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

なお、図2に示す暗号処理手段150は、1つのワンチップLSIとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

[キー配信構成としてのツリー（木）構造について]

次に、図1に示すコンテンツ配信側10からコンテンツ受信側20の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成及びデータ配信構成を図3を用いて説明する。

図3の最下段に示すナンバ0～15がコンテンツ受信側20の個々のデバイスである。すなわち図3に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーからなるキーセットをメモリに格納する。図3の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

図3に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ

内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、図3の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、メッセージデータ配信手段として機能する。

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行うプロバイダ、決済機関等のメッセージデータ配信手段によってグループ毎に管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス0, 1, 2, 3のみに提供することが可能となる。例えば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキー: Kconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

また、ある時点 t において、デバイス3の所有する鍵： $K0011$ ， $K001$ ， $K00$ ， $K0$ ， KR が攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0，1，2，3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー： $K001$ ， $K00$ ， $K0$ ， KR をそれぞれ新たな鍵 $K(t)001$ ， $K(t)00$ ， $K(t)0$ ， $K(t)R$ に更新し、デバイス0，1，2にその更新キーを伝える必要がある。ここで、 $K(t)aaa$ は、鍵 $Kaaa$ の世代（Generation）： t の更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図4Aに示す有効化キーブロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス0，1，2に供給することによって実行される。なお、有効化キーブロック（EKB）は、図3に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（EKB）は、キー更新ブロック（KRB：Key Renewal Block）と呼ばれることもある。

図4Aに示す有効化キーブロック（EKB）には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4A及び図4Bの例は、図3に示すツリー構造中のデバイス0，1，2において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0，デバイス1は、更新ノードキーとして $K(t)00$ ， $K(t)0$ ， $K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001$ ， $K(t)00$ ， $K(t)0$ ， $K(t)R$ が必要である。

図4AのEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た K

(t) 001を用いて、図4Aの下から2段目の暗号化キーEnc(K(t) 001, K(t) 00)を復号可能となり、更新ノードキーK(t) 00を得ることができる。以下順次、図4Aの上から2段目の暗号化キーEnc(K(t) 00, K(t) 0)を復号し、更新ノードキーK(t) 0、図4Aの上から1段目の暗号化キーEnc(K(t) 0, K(t) R)を復号しK(t) Rを得る。一方、デバイスK0000、K0001は、ノードキーK000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t) 00、K(t) 0、K(t) Rである。デバイスK0000、K0001は、図4Aの上から3段目の暗号化キーEnc(K000, K(t) 00)を復号しK(t) 00を取得し、以下、図4Aの上から2段目の暗号化キーEnc(K(t) 00, K(t) 0)を復号し、更新ノードキーK(t) 0、図4Aの上から1段目の暗号化キーEnc(K(t) 0, K(t) R)を復号しK(t) Rを得る。このようにして、デバイス0, 1, 2は更新した鍵K(t) Rを得ることができる。なお、図4Aのインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図3に示すツリー構造の上位段のノードキー：K(t) 0, K(t) Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図4Bの有効化キーブロック(EKB)を用いることで、更新ノードキーK(t) 00をデバイス0, 1, 2に配布することができる。

図4Bに示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツキーK(t) conが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t) 00を用いて新たな共通の更新コンテンツキー：K(t) conを暗号化したデータEnc(K(t) 00, K(t) con)を図4Bに示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス0, 1, 2はEKBを処理して得たK(t) 00を用いて

上記暗号文を復号すれば、 t 時点でのコンテンツキー $K(t)_{con}$ を得ることが可能になる。

[EKBを使用したコンテンツキーの配布]

図5に、 t 時点でのコンテンツキー $K(t)_{con}$ を得る処理例として、 $K(t)_{00}$ を用いて新たな共通のコンテンツキー $K(t)_{con}$ を暗号化したデータ $Enc(K(t)_{00}, K(t)_{con})$ と図4Bに示すEKBとを記録媒体を介して受領したデバイス0の処理を示す。すなわちEKBによる暗号化メッセージデータをコンテンツキー $K(t)_{con}$ とした例である。

図5に示すように、デバイス0は、記録媒体に格納されている世代： t 時点のEKBと自分が予め格納しているノードキー K_{000} を用いて上述したと同様のEKB処理により、ノードキー $K(t)_{00}$ を生成する。さらに、復号した更新ノードキー $K(t)_{00}$ を用いて更新コンテンツキー $K(t)_{con}$ を復号して、後にそれを使用するために自分だけが持つリーフキー K_{0000} で暗号化して格納する。

[EKBのフォーマット]

図6に有効化キーブロック(EKB)のフォーマット例を示す。バージョン601は、有効化キーブロック(EKB)のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポイント603は、有効化キーブロック(EKB)中のデータ部の位置を示すポイントであり、タグポイント604はタグ部の位置、署名ポイント605は署名の位置を示すポイントである。

データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

タグ部607は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図7A乃至図7Cを用いて説明する。図7A乃至図7Cでは、データとして先に図4Aで説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図7B

に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図7Aに示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、全てのデータにタグが設定され、図7Cに示すデータ列、及びタグ列が構成される。

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy) \dots$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図4A及び図4Bで説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : $Enc(K(t)0, K(t)root)$

00 : $Enc(K(t)00, K(t)0)$

000 : $Enc(K(t)000, K(t)00)$

...のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

図6に戻って、EKBフォーマットについてさらに説明する。署名(Signature)は、有効化キーブロック(EKB)を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイ

スは署名検証によって正当な有効化キープロック (EKB) 発行者が発行した有効化キープロック (EKB) であることを確認する。

[EKBを使用したコンテンツキー及びコンテンツの配信]

上述の例では、コンテンツキーのみをEKBとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、EKBによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

図8A及び図8Bにこのデータ構成を示す。図8Aに示す構成において、Enc(Kcon, content) 801は、コンテンツ (Content) をコンテンツキー (Kcon) で暗号化したデータであり、Enc(KEK, Kcon) 802は、コンテンツキー (Kcon) をコンテンツキー暗号キー (KEK: Key Encryption Key) で暗号化したデータであり、Enc(EKB, KEK) 803は、コンテンツキー暗号キーKEKを有効化キープロック (EKB) によって暗号化したデータであることを示す。

ここで、コンテンツキー暗号キーKEKは、図3で示すノードキー (K000, K00...)、あるいはルートキー (KR) 自体であってもよく、またノードキー (K000, K00...)、あるいはルートキー (KR) によって暗号化されたキーであってもよい。

図8Bは、複数のコンテンツがメディアに記録され、それぞれが同じEnc(EKB, KEK) 805を利用している場合の構成例を示す、このような構成においては、各データに同じEnc(EKB, KEK) を付加することなく、Enc(EKB, KEK) にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

図9にコンテンツキー暗号キーKEKを、図3に示すノードキーK00を更新した更新ノードキーK(t)00として構成した場合の例を示す。この場合、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク (排除) されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2に対して図9に示す有効化キープロック (EKB) と、コンテンツキー (Kcon) をコンテンツキー暗号キー (KEK=K(t)00) で暗号化した

データと、コンテンツ (content) をコンテンツキー (K c o n) で暗号化したデータとを配信することにより、デバイス 0, 1, 2 はコンテンツを得ることができる。

図 9 の右側には、デバイス 0 における復号手順を示してある。デバイス 0 は、まず、受領した有効化キーブロックから自身の保有するリーフキー $K 0 0 0$ を用いた復号処理により、コンテンツキー暗号キー ($K E K = K (t) 0 0$) を取得する。次に、 $K (t) 0 0$ による復号によりコンテンツキー $K c o n$ を取得し、さらにコンテンツキー $K c o n$ によりコンテンツの復号を行う。これらの処理により、デバイス 0 はコンテンツを利用可能となる。デバイス 1, 2 においても各々異なる処理手順で $E K B$ を処理することにより、コンテンツキー暗号キー ($K E K = K (t) 0 0$) を取得することが可能となり、同様にコンテンツを利用することが可能となる。

図 3 に示す他のグループのデバイス 4, 5, 6... は、この同様のデータ ($E K B$) を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー ($K E K = K (t) 0 0$) を取得することができない。同様にリボークされたデバイス 3 においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー ($K E K = K (t) 0 0$) を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

このように、 $E K B$ を利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

なお、有効化キーブロック ($E K B$)、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック ($E K B$)、コンテンツキー、暗号化コンテンツを DVD、CD 等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック ($E K B$) の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ

利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

図10に記録媒体に暗号化コンテンツとともに有効化キープブロック(EKB)を格納した構成例を示す。図10に示す例においては、記録媒体にコンテンツC1～C4が格納され、さらに各格納コンテンツに対応するの有効化キープブロック(EKB)を対応付けたデータが格納され、さらにバージョンMの有効化キープブロック(EKB__M)が格納されている。例えばEKB__1はコンテンツC1を暗号化したコンテンツキーKcon1を生成するのに使用され、例えばEKB__2はコンテンツC2を暗号化したコンテンツキーKcon2を生成するのに使用される。この例では、バージョンMの有効化キープブロック(EKB__M)が記録媒体に格納されており、コンテンツC3、C4は有効化キープブロック(EKB__M)に対応付けられているので、有効化キープブロック(EKB__M)の復号によりコンテンツC3、C4のコンテンツキーを取得することができる。EKB__1、EKB__2はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なEKB__1、EKB__2を取得することが必要となる。

図11A及び図11Bに、複数のデバイス間でコンテンツキーが流通する場合のEKBを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。図11Aが従来構成であり、図11Bが本発明の有効化キープブロック(EKB)を利用した例である。なお、図11A及び図11BにおいてKa(Kb)は、KbをKaで暗号化したデータであることを示す。

図11Aに示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーKsesを共有するために各デバイス間において、認証処理及び鍵交換処理(AKE: Authentication and Key Exchange)を実行し、認証が成立したことを条件としてセッションキーKsesでコンテンツキーKconを暗号化して送信する処理を行っていた。

例えば図11AのPCにおいては、受信したセッションキーで暗号化したコンテンツキーKses(Kcon)をセッションキーで復号してKconを得ることが可能であり、さらに取得したKconをPC自体の保有する保存キーKst

rで暗号化して自身のメモリに保存することが可能となる。

図11Aにおいて、コンテンツプロバイダは、図11Aの記録デバイス1101にのみデータを利用可能な形で配信したい場合でも、間にPC、再生装置が存在する場合は、図11Aに示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要となる。また、間に介在するPC、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

一方、図11Bの下段に示す有効化キーブロック(EKB)を利用した例においては、コンテンツプロバイダから有効化キーブロック(EKB)と、有効化キーブロック(EKB)の処理によって得られるノードキー、又はルートキーによってコンテンツキーKconを暗号化したデータ(図の例ではKroot(Kcon))を配信することにより、配信したEKBの処理が可能な機器においてのみコンテンツキーKconを復号して取得することが可能になる。

従って、例えば図11Bの右端にのみ利用可能な有効化キーブロック(EKB)を生成して、その有効化キーブロック(EKB)と、そのEKB処理によって得られるノードキー、又はルートキーによってコンテンツキーKconを暗号化したデータを併せて送ることにより、間に存在するPC、再生機器等は、自身の有するリーフキー、ノードキーによっては、EKBの処理を実行することができない。従って、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーKconの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

PC、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キーブロック(EKB)を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

[有効化キーブロック(EKB)を使用した認証キーの配信(共通鍵方式)]

上述の有効化キーブロック(EKB)を使用したデータあるいはキーの配信に

において、デバイス間で転送される有効化キープロック (EKB) 及びコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝送路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理及び鍵交換処理を実行することが有効な手段である。ここでは、この認証処理及び鍵交換処理を実行する際に使用する認証キー K_{ake} を上述の有効化キープロック (EKB) を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわち EKB による暗号化メッセージデータを認証キーとした例である。

図 12 に、共通鍵暗号方式を用いた相互認証方法 (ISO/IEC 9798-2) を示す。図 12 においては、共通鍵暗号方式として DES を用いているが、共通鍵暗号方式であれば他の方式も可能である。図 12 において、まず、B が 64 ビットの乱数 R_b を生成し、 R_b 及び自己の ID である $ID(b)$ を A に送信する。これを受信した A は、新たに 64 ビットの乱数 R_a を生成し、 R_a 、 R_b 、 $ID(b)$ の順に、DES の CBC モードで鍵 K_{ab} を用いてデータを暗号化し、B に返送する。なお、鍵 K_{ab} は、A 及び B に共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。DES の CBC モードを用いた鍵 K_{ab} による暗号化処理は、例えば DES を用いた処理においては、初期値と R_a との排他的論理和を求め、DES 暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_1 を生成し、続けて暗号文 E_1 と R_b との排他的論理和を求め、DES 暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_2 を生成し、さらに、暗号文 E_2 と $ID(b)$ との排他的論理和を求め、DES 暗号化部において、鍵 K_{ab} を用いて暗号化して生成した暗号文 E_3 とによって送信データ (Token-AB) を生成する。

これを受信した B は、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵 K_{ab} (認証キー) で復号化する。受信データの復号化方法は、まず、暗号文 E_1 を認証キー K_{ab} で復号化し、乱数 R_a を得る。次に、暗号文 E_2 を認証キー K_{ab} で復号化し、その結果と E_1 の排他的論理和を求め、 R_b を得る。最後に、暗号文 E_3 を認証キー K_{ab} で復号化し、その結果と E_2

の排他的論理和を求め、 $ID(b)$ を得る。こうして得られた R_a 、 R_b 、 $ID(b)$ の内、 R_b 及び $ID(b)$ が、 B が送信したものと一致するか検証する。この検証に通った場合、 B は A を正当なものとして認証する。

次に B は、認証後に使用するセッションキー(K_{ses})を生成する(生成方法は、乱数を用いる)。そして、 R_b 、 R_a 、 K_{ses} の順に、 DES のCBCモードで認証キー K_{ab} を用いて暗号化し、 A に返送する。

これを受信した A は、受信データを認証キー K_{ab} で復号化する。受信データの復号化方法は、 B の復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b 及び R_a が、 A が送信したものと一致するか検証する。この検証に通った場合、 A は B を正当なものとして認証する。互いに相手を認証した後には、セッションキー K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

上述の認証処理においては、 A 、 B は共通の認証キー K_{ab} を共有する。この共通鍵 K_{ab} を上述の有効化キーブロック(EKB)を使用してデバイスに配信する。

例えば、図12の例では、 A 、又は B のいずれかが他方が復号可能な有効化キーブロック(EKB)を生成して生成した有効化キーブロック(EKB)によって認証キー K_{ab} を暗号化して、他方に送信する構成としてもよいし、あるいは第3者がデバイス A 、 B に対して双方が利用可能な有効化キーブロック(EKB)を生成してデバイス A 、 B に対して生成した有効化キーブロック(EKB)によって認証キー K_{ab} を暗号化して配信する構成としてもよい。

図13及び図14に複数のデバイスに共通の認証キー K_{ake} を有効化キーブロック(EKB)によって配信する構成例を示す。図13はデバイス0, 1, 2, 3に対して復号可能な認証キー K_{ake} を配信する例、図14はデバイス0, 1, 2, 3中のデバイス3をリボーク(排除)してデバイス0, 1, 2に対してのみ復号可能な認証キーを配信する例を示す。

図13の例では、更新ノードキー $K(t)00$ によって、認証キー K_{ake} を

暗号化したデータとともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)00$ を復号可能な有効化キープブロック(EKB)を生成して配信する。それぞれのデバイスは、図13の右側に示すようにまず、EKBを処理(復号)することにより、更新されたノードキー $K(t)00$ を取得し、次に、取得したノードキー $K(t)00$ を用いて暗号化された認証キー: $Enc(K(t)00, Kake)$ を復号して認証キー $Kake$ を得ることが可能となる。

その他のデバイス4, 5, 6, 7...は同一の有効化キープブロック(EKB)を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキー $K(t)00$ を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

一方、図14の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク(排除)されているとして、他のグループのメンバー、すなわち、デバイス0, 1, 2に対してのみ復号可能な有効化キープブロック(EKB)を生成して配信した例である。図14に示す有効化キープブロック(EKB)と、認証キー($Kake$)をノードキー($K(t)00$)で暗号化したデータを配信する。

図14の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープブロックから自身の保有するリーフキー又はノードキーを用いた復号処理により、更新ノードキー($K(t)00$)を取得する。次に、 $K(t)00$ による復号により認証キー $Kake$ を取得する。

図3に示す他のグループのデバイス4, 5, 6...は、この同様のデータ(EKB)を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー($K(t)00$)を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー($K(t)00$)を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

このように、EKBを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可

能となる。

〔公開鍵認証と有効化キープロック (E K B) を使用したコンテンツキーの配信〕

次に、公開鍵認証と有効化キープロック (E K B) を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である 160 ビット長の楕円曲線暗号を用いた相互認証方法を、図 15 を用いて説明する。図 15 において、公開鍵暗号方式として E C C を用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも 160 ビットでなくてもよい。図 15 において、まず B が、64 ビットの乱数 R_b を生成し、A に送信する。これを受信した A は、新たに 64 ビットの乱数 R_a 及び素数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v (X 座標と Y 座標) に対する電子署名 $A.Sig$ を生成し、A の公開鍵証明書とともに B に返送する。ここで、 R_a 及び R_b はそれぞれ 64 ビット、 A_v の X 座標と Y 座標がそれぞれ 160 ビットであるので、合計 448 ビットに対する電子署名を生成する。

A の公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 $A.Sig$ を受信した B は、A が送信してきた R_b が、B が生成したものと一致するか検証する。その結果、一致していた場合には、A の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、A の公開鍵を取り出す。そして、取り出した A の公開鍵を用い電子署名 $A.Sig$ を検証する。

次に、B は、素数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v (X 座標と Y 座標) に対する電子署名 $B.Sig$ を生成し、B の公開鍵証明書とともに A に返送する。

B の公開鍵証明書、 R_b 、 R_a 、 A_v 、電子署名 $B.Sig$ を受信した A は、B が送信してきた R_a が、A が生成したものと一致するか検証する。その結果、一致していた場合には、B の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、B の公開鍵を取り出す。そして、取り出した B の公開鍵を用い電子署名 $B.Sig$ を検証する。電子署名の検証に成功した後、A は B を正当なものとして認証する。

両者が認証に成功した場合には、 B は $B_k \times A_v$ (B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要) を計算し、 A は $A_k \times B_v$ を計算し、これら点の X 座標の下位64ビットをセッションキーとして以降の通信に使用する(共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。もちろん、 Y 座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

図16に公開鍵認証と有効化キーブロック(EKB)を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとPC間において図15で説明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なEKBを生成して、更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)とをPC間の認証処理において生成したセッションキーKsesで暗号化してPCに送信する。

PCはセッションキーで暗号化された[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]をセッションキーで復号した後、再生装置、記録媒体に送信する。

再生装置、記録媒体は、自身の保有するノードキー又はリーフキーによって[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]を復号することによってコンテンツキーKconを取得する。

この構成によれば、コンテンツプロバイダとPC間での認証を条件として[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

[プログラムコードの有効化キーブロック(EKB)を使用した配信]

上述した例では、コンテンツキー、認証キー等を有効化キーブロック(EK

B) を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キープブロック (EKB) を用いて配信する構成も可能である。すなわち EKB による暗号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

図 17 にプログラムコードを有効化キープブロック (EKB) の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス 1701 は、デバイス 1702 の有するノードキー、リーフキーによって復号可能な有効化キープブロック (EKB) と、有効化キープブロック (EKB) に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス 1702 に送信する。デバイス 1702 は受信した EKB を処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコードを得る。

図 17 に示す例では、さらに、デバイス 1702 において取得したプログラムコードによる処理を実行して、その結果をデバイス 1701 に返して、デバイス 1701 がその結果に基づいて、さらに処理を続行する例を示している。

このように有効化キープブロック (EKB) と、有効化キープブロック (EKB) に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図 3 で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

[送信コンテンツに対するチェック値 (ICV: Integrity Check Value) を対応させる構成]

次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値 (ICV) を生成して、コンテンツに対応付けて、ICV の計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

コンテンツのインテグリティ・チェック値 (ICV) は、例えばコンテンツに対するハッシュ関数を用いて計算され、 $ICV = hash(K_{icv}, C1, C2, \dots)$ によって計算される。K_{icv} は ICV 生成キーである。C1, C2 はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号 (MAC: Message authentication Code) が使用される。

D E S 暗号処理構成を用いた M A C 値生成例を図 1 8 に示す。図 1 8 の構成に示すように対象となるメッセージを 8 バイト単位に分割し、(以下、分割されたメッセージを M 1、M 2、・・・、M N とする)、まず、初期値 (Initial Value (以下、I V とする)) と M 1 の排他的論理和を求める (その結果を I 1 とする)。次に、I 1 を D E S 暗号化部に入れ、鍵 (以下、K 1 とする) を用いて暗号化する (出力を E 1 とする)。続けて、E 1 及び M 2 の排他的論理和を求め、その出力 I 2 を D E S 暗号化部へ入れ、鍵 K 1 を用いて暗号化する (出力 E 2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E N がメッセージ認証符号 (M A C (Message Authentication Code)) となる。

このようなコンテンツの M A C 値と I C V 生成キーにハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値 (I C V) が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成した I C V と、新たにコンテンツに基づいて生成した I C V とを比較して同一の I C V が得られればコンテンツに改竄のないことが保証され、I C V が異なれば、改竄があったと判定される。

[チェック値 (I C V) の生成キー K i c v を E K B によって配布する構成]

次に、コンテンツのインテグリティ・チェック値 (I C V) 生成キーである K i c v を上述の有効化キーブロックによって送付する構成について説明する。すなわち E K B による暗号化メッセージデータをコンテンツのインテグリティ・チェック値 (I C V) 生成キーとした例である。

図 1 9 及び図 2 0 に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キー K i c v を有効化キーブロック (E K B) によって配信する構成例を示す。図 1 9 はデバイス 0, 1, 2, 3 に対して復号可能なチェック値生成キー K i c v を配信する例、図 2 0 はデバイス 0, 1, 2, 3 中のデバイス 3 をリボーク (排除) してデバイス 0, 1, 2 に対してのみ復号可能なチェック値生成キー K i c v を配信する例を示す。

図19の例では、更新ノードキー $K(t)00$ によって、チェック値生成キー K_{icv} を暗号化したデータとともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)00$ を復号可能な有効化キーブロック(EKB)を生成して配信する。それぞれのデバイスは、図19の右側に示すようにまず、EKBを処理(復号)することにより、更新されたノードキー $K(t)00$ を取得し、次に、取得したノードキー $K(t)00$ を用いて暗号化されたチェック値生成キー: $Enc(K(t)00, K_{icv})$ を復号してチェック値生成キー K_{icv} を得ることが可能となる。

その他のデバイス4, 5, 6, 7...は同一の有効化キーブロック(EKB)を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキー $K(t)00$ を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

一方、図20の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク(排除)されているとして、他のグループのメンバー、すなわち、デバイス0, 1, 2に対してのみ復号可能な有効化キーブロック(EKB)を生成して配信した例である。図20に示す有効化キーブロック(EKB)と、チェック値生成キー(K_{icv})をノードキー($K(t)00$)で暗号化したデータを配信する。

図20の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受信した有効化キーブロックから自身の保有するリーフキー又はノードキーを用いた復号処理により、更新ノードキー($K(t)00$)を取得する。次に、 $K(t)00$ による復号によりチェック値生成キー K_{icv} を取得する。

図3に示す他のグループのデバイス4, 5, 6...は、この同様のデータ(EKB)を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー($K(t)00$)を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー($K(t)00$)を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

このように、EKBを利用したチェック値生成キーの配送を用いれば、データ

量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

このようなコンテンツのインテグリティ・チェック値 (ICV) を用いることにより、EKBと暗号化コンテンツの不正コピーを排除することができる。例えば図21A及び図21Bに示すように、コンテンツC1とコンテンツC2とをそれぞれのコンテンツキーを取得可能な有効化キーブロック (EKB) とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化コンテンツのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できることになる。

図21Bに示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値 (ICV (C1, C2)) を格納する構成とする。なお、(ICV (C1, C2)) は、コンテンツC1とコンテンツC2にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値である $ICV = hash(K_{icv}, C1, C2)$ を示している。図21Bの構成において、メディア1には正当にコンテンツ1とコンテンツ2が格納され、コンテンツC1とコンテンツC2に基づいて生成されたインテグリティ・チェック値 (ICV (C1, C2)) が格納される。また、メディア2には正当にコンテンツ1が格納され、コンテンツC1に基づいて生成されたインテグリティ・チェック値 (ICV (C1)) が格納される。この構成において、メディア1に格納された {EKB, コンテンツ2} をメディア2にコピーしたとすると、メディア2で、コンテンツチェック値を新たに生成するとICV (C1, C2) が生成されることになり、メディアに格納されている $K_{icv} (C1)$ と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにICVチェックを実行して、生成ICVと格納ICVの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値 (ICV) を書き換えカウンタを含めたデータに基づいて生成する構成として

もよい。すなわち $ICV = \text{hash}(K_{icv}, \text{counter} + 1, C_1, C_2, \dots)$ によって計算する構成とする。ここで、カウンタ ($\text{counter} + 1$) は、ICVの書き換え毎に1つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

さらに、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツとは別のメディア上に格納する構成としてもよい。

例えば、読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値 (ICV) を格納するとICVの書き換えが不正なユーザによりなされる可能性があり、ICVの安全性が保てないおそれがある。このような場合、ホストマシン上の安全なメディアにICVを格納して、コンテンツのコピーコントロール (例えばcheck-in/check-out、move) にICVを使用する構成とすることにより、ICVの安全な管理及びコンテンツの改竄チェックが可能となる。

この構成例を図22に示す。図22では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値 (ICV) を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア2202に格納し、ユーザによる不正なインテグリティ・チェック値 (ICV) の書き換えを防止した例である。このような構成として、例えばメディア2201を装着したデバイスがメディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

[階層ツリー構造のカテゴリ分類]

暗号鍵をルートキー、ノードキー、リーフキー等、図3の階層ツリー構造として構成し、コンテンツキー、認証キー、ICV生成キー、あるいはプログラムコード、データ等を有効化キーブロック (EKB) とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デ

バイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

図23に階層ツリー構造のカテゴリの分類の一例を示す。図23において、階層ツリー構造の最上段には、ルートキーK r o o t 2 3 0 1が設定され、以下の中間段にはノードキー2 3 0 2が設定され、最下段には、リーフキー2 3 0 3が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

ここで、一例として最上段から第M段目のあるノードをカテゴリノード2 3 0 4として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノード及びリーフとする。

例えば図23の第M段目の1つのノード2 3 0 5にはカテゴリ「メモリスティック（商標）」が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノード又はリーフとして設定される。すなわち、ノード2 3 0 5以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、及びリーフの集合として定義する。

さらに、M段から数段分下位の段をサブカテゴリノード2 3 0 6として設定することができる。例えば図に示すようにカテゴリ「メモリスティック」ノード2 3 0 5の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、「再生専用器」のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード2 3 0 6以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2 3 0 7が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる「PHS」ノード2 3 0 8と「携帯電話」ノード2 3 0 9を設定することができる。

さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つの

カテゴリノードをゲーム機器メーカーの販売するゲーム機器X Y Z専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器X Y Zにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（E K B）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（E K B）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

〔簡略E K Bによるキー配信構成（1）〕

先に説明した例えば図3のツリー構成において、キー、例えばコンテンツキーを所定デバイス（リーフ）宛に送付する場合、キー配布先デバイスの所有しているリーフキー、ノードキーを用いて復号可能な有効化キーブロック（E K B）を生成して提供する。例えば図24Aに示すツリー構成において、リーフを構成するデバイスa, g, jに対してキー、例えばコンテンツキーを送信する場合、a, g, jの各ノードにおいて復号可能な有効化キーブロック（E K B）を生成して配信する。

例えば更新ルートキーK (t) r o o tでコンテンツキーK (t) c o nを暗号化処理し、E K Bとともに配信する場合を考える。この場合、デバイスa, g, jは、それぞれが図24Bに示すリーフ及びノードキーを用いて、E K Bの処理を実行してK (t) r o o tを取得し、取得した更新ルートキーK (t) r o o tによってコンテンツキーK (t) c o nの復号処理を実行してコンテンツキーを得る。

この場合に提供される有効化キーブロック（E K B）の構成は、図25に示す

ようになる。図 2 5 に示す有効化キーブロック (E K B) は、先の図 6 で説明した有効化キーブロック (E K B) のフォーマットにしたがって構成されたものであり、データ (暗号化キー) と対応するタグとを持つ。タグは、先に図 7 A 乃至図 7 C を用いて説明したように左 (L)、右 (R)、それぞれの方向にデータがあれば 0、無ければ 1 を示している。

有効化キーブロック (E K B) を受領したデバイスは、有効化キーブロック (E K B) の暗号化キーとタグに基づいて、順次暗号化キーの復号処理を実行して上位ノードの更新キーを取得していく。図 2 5 に示すように、有効化キーブロック (E K B) は、ルートからリーフまでの段数 (デプス) が多いほど、そのデータ量は増加していく。段数 (デプス) は、デバイス (リーフ) 数に応じて増大するものであり、キーの配信先となるデバイス数が多い場合は、E K B のデータ量がさらに増大することになる。

このような有効化キーブロック (E K B) のデータ量の削減を可能とした構成について説明する。図 2 6 A 及び図 2 6 B は、有効化キーブロック (E K B) をキー配信デバイスに応じて簡略化して構成した例を示すものである。

図 2 5 と同様、リーフを構成するデバイス a, g, j に対してキー、例えばコンテンツキーを送信する場合を想定する。図 2 6 A に示すように、キー配信デバイスによってのみ構成されるツリーを構築する。この場合、図 2 4 B に示す構成に基づいて新たなツリー構成として図 2 6 B のツリー構成が構築される。K r o o t から K j までは全く分岐がなく 1 つの枝のみが存在すればよく、K r o o t から K a 及び K g に至るためには、K 0 に分岐点を構成するのみで、2 分岐構成の図 2 6 A のツリーが構築される。

図 2 6 A に示すように、ノードとして K 0 のみを持つ簡略化したツリーが生成される。更新キー配信のための有効化キーブロック (E K B) は、これらの簡略ツリーに基づいて生成する。図 2 6 A に示すツリーは、有効化キーブロック (E K B) を復号可能な末端ノード又はリーフを最下段とした 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーである。更新キー配信のための有効化キーブロック (E K B) は、この再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成される。

先の図25で説明した有効化キーブロック (EKB) は、各リーフ a, g, j から K_{root} に至るまでの全てのキーを暗号化したデータを格納していたが、簡略化 EKB は、簡略化したツリーを構成するノードについてのみの暗号化データを格納する。図26Bに示すようにタグは3ビット構成を有する。第1及び第2ビットは、図25の例と、同様の意味を持ち、左 (L)、右 (R)、それぞれの方向にデータがあれば0、無ければ1を示す。第3番目のビットは、EKB内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は1、データが無い場合は、0として設定される。

データ通信網、あるいは記憶媒体に格納されてデバイス (リーフ) に提供される有効化キーブロック (EKB) は、図26Bに示すように、図25に示す構成に比較すると、データ量が大幅に削減されたものとなる。図26A及び図26Bに示す有効化キーブロック (EKB) を受領した各デバイスは、タグの第3ビットに1が格納された部分のデータのみを順次復号することにより、所定の暗号化キーの復号を実現することができる。例えばデバイス a は、暗号化データ $Enc(K_a, K(t)_0)$ をリーフキー K_a で復号して、ノードキー $K(t)_0$ を取得して、ノードキー $K(t)_0$ によって暗号化データ $Enc(K(t)_0, K(t)_{root})$ を復号して $K(t)_{root}$ を取得する。デバイス j は、暗号化データ $Enc(K_j, K(t)_{root})$ をリーフキー K_j で復号して、 $K(t)_{root}$ を取得する。

このように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフ及びノードのキーのみを用いて有効化キーブロック (EKB) を生成することにより、少ないデータ量の有効化キーブロック (EKB) を生成することが可能となり、有効化キーブロック (EKB) のデータ配信が効率的に実行可能となる。

[簡略 EKB によるキー配信構成 (2)]

図26A及び図26Bで示した簡略化したツリーに基づいて生成される有効化キーブロック (EKB) をさらに、簡略化してデータ量を削減し、効率的な処理を可能とした構成について説明する。

図26A及び図26Bを用いて説明した構成は、有効化キーブロック (EK

B) を復号可能な末端ノード又はリーフを最下段とした2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーであった。更新キー配信のための有効化キーブロック (EKB) は、この再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成される。

図26Aに示す再構築階層ツリーは、リーフa, g, jにおいて更新ルートキー $K(t)_{root}$ を取得可能とするため、図26Bに示す有効化キーブロック (EKB) を配信する。図26Bの有効化キーブロック (EKB) の処理において、リーフjは、 $Enc(K_j, K(t)_{root})$ の1回の復号処理によりルートキー: $K(t)_{root}$ を取得できる。しかし、リーフa, gは、 $Enc(K_a, K(t)_0)$ 又は、 $Enc(K_g, K(t)_0)$ の復号処理により $K(t)_0$ を得た後、さらに、 $Enc(K(t)_0, K(t)_{root})$ の復号処理を実行してルートキー: $K(t)_{root}$ を取得する。すなわち、リーフa, gは、2回の復号処理を実行することが必要となる。

図26A及び図26Bの簡略化した再構築階層ツリーは、ノード K_0 がその下位リーフa, gの管理ノードとして独自の管理を実行している場合、例えば後述するサブルート・ノードとして、下位リーフの管理を実行している場合には、リーフa, gが更新キーを取得したことを確認する意味で有効であるが、ノード K_0 が下位リーフの管理を行っていない場合、あるいは行なっていたとしても、上位ノードからの更新キー配信を許容している場合には、図26Aに示す再構築階層ツリーをさらに簡略化して、ノード K_0 のキーを省略して有効化キーブロック (EKB) を生成して配信してもよい。

図27A及び図27Bに、このような有効化キーブロック (EKB) の構成を示す。図26A及び図26Bと同様、リーフを構成するデバイスa, g, jに対してキー、例えばコンテンツキーを送信する場合を想定する。図27Aに示すように、ルート K_{root} と各リーフa, g, jを直接接続したツリーを構築する。

図27Aに示すように、図26Aに示す再構築階層ツリーからノード K_0 が省かれた簡略化したツリーが生成される。更新キー配信のための有効化キーブロック (EKB) は、これらの簡略ツリーに基づいて生成する。図27Aに示すツリーは、有効化キーブロック (EKB) を復号可能なリーフをとルートとを直接結

ぶパスのみによって再構築される再構築階層ツリーである。更新キー配信のための有効化キーブロック (EKB) は、この再構築階層ツリーのリーフに対応するキーのみに基づいて構成される。

なお、図 27 A の例は、末端をリーフとした構成例であるが、例えば最上位ノードか複数の中位、下位ノードに対してキーを配信する場合も、最上位ノードと中位、下位ノードとを直接接続した簡略化ツリーに基づいて有効化キーブロック (EKB) を生成してキー配信を実行することが可能である。このように、再構築階層ツリーは、簡略化したツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノード又はリーフとを直接、接続した構成を持つ。この簡略化ツリーでは、頂点ノードからの分岐は 2 に限らず、配信ノード又はリーフ数に応じて 3 以上の多分岐を持つツリーとして構成することが可能である。

先の図 25 で説明した有効化キーブロック (EKB) は、各リーフ a, g, j から K r o o t に至るまでの全てのキーを暗号化したデータを格納し、図 26 A 及び図 26 B で説明した有効化キーブロック (EKB) は、リーフ a, g, j のリーフキー、a, g の共通ノードとしての K0、さらに、ルートキーを格納した構成であったが、図 27 A に示す簡略化階層ツリーに基づく有効化キーブロック (EKB) は、ノード K0 のキーを省略したので、図 27 B に示すように、さらにデータ量の少ない有効化キーブロック (EKB) となる。

図 27 B の有効化キーブロック (EKB) は、図 26 B の有効化キーブロック (EKB) と同様、3 ビット構成のタグを有する。第 1 及び第 2 ビットは、図 26 A 及び図 26 B で説明したと同様、左 (L)、右 (R)、それぞれの方向にデータがあれば 0、無ければ 1 を示す。第 3 番目のビットは、EKB 内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は 1、データが無い場合は、0 として設定される。

図 27 B の有効化キーブロック (EKB) において、各リーフ a, g, j は、 $Enc(Ka, K(t)root)$ 、又は $Enc(Kg, K(t)root)$ $Enc(Kj, K(t)root)$ の 1 回の復号処理によりルートキー: $K(t)root$ を取得できる。

このように簡略化された再構築ツリーの最上位ノードと、ツリーを構成する末

端ノード又はリーフとを直接、接続した構成を持つツリーに基づいて生成される有効化キーブロック（EKB）は、図27Bに示すように、再構築階層ツリーの頂点ノード及び末端ノード又はリーフに対応するキーのみに基づいて構成される。

図26A及び図26B又は図27A及び図27Bで説明した有効化キーブロック（EKB）のように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフのみ、あるいはリーフと共通ノードのキーのみを用いて有効化キーブロック（EKB）を生成することにより、少ないデータ量の有効化キーブロック（EKB）を生成することが可能となり、有効化キーブロック（EKB）のデータ配信が効率的に実行可能となる。

なお、簡略化した階層ツリー構成は、後段で説明するエンティティ単位のEKB管理構成において特に有効に活用可能である。エンティティは、キー配信構成としてのツリー構成を構成するノードあるいはリーフから選択した複数のノードあるいはリーフの集合体ブロックである。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。1つのエンティティには、ある共通のカテゴリに分類されるデバイスが集まっており、例えば複数のエンティティの頂点ノード（サブルート）によって上述したと同様の簡略化したツリーを再構築してEKBを生成することにより、選択されたエンティティに属するデバイスにおいて復号可能な簡略化された有効化キーブロック（EKB）の生成、配信が可能となる。エンティティ単位の管理構成については後段で詳細に説明する。

なお、このような有効化キーブロック（EKB）は、光ディスク、DVD等の情報記録媒体に格納した構成とすることが可能である。例えば、上述の暗号化キーデータによって構成されるデータ部と、暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（EKB）にさらに、更新ノードキーによって暗号化したコンテンツ等のメッセージデータとを格納した情報記録媒体を各デバイスに提供する構成が可能である。デバイスは

有効化キーブロック (EKB) に含まれる暗号化キーデータをタグ部の識別データにしたがって順次抽出して復号し、コンテンツの復号に必要なキーを取得してコンテンツの利用を行うことが可能となる。もちろん、有効化キーブロック (EKB) をインターネット等のネットワークを介して配信する構成としてもよい。

[エンティティ単位のEKB管理構成]

次に、キー配信構成としてのツリー構成を構成するノードあるいはリーフを、複数のノードあるいはリーフの集合としてのブロックで管理する構成について説明する。なお、複数のノードあるいはリーフの集合としてのブロックを以下エンティティと呼ぶ。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。

エンティティについて、図28乃至図28Cを用いて説明する。図28Aはツリーのエンティティ単位での管理構成を説明する図である。1つのエンティティは図では、三角形として示し、例えば1エンティティ2701内には、複数のノードが含まれる。1エンティティ内のノード構成を示すのが図28Bである。1つのエンティティは、1つのノードを頂点とした複数段の2分岐形ツリーによって構成される。以下、エンティティの頂点ノード2702をサブルートと呼ぶ。

ツリーの末端は、図28Cに示すようにリーフ、すなわちデバイスによって構成される。デバイスは、複数デバイスをリーフとし、サブルートである頂点ノード2702を持つツリーによって構成されるいずれかのエンティティに属する。

図28Aから理解されるように、エンティティは、階層構造を持つ。この階層構造について、図29A乃至図29Cを用いて説明する。

図29Aは、階層構造を簡略化して説明するための図であり、Krootから数段下の段にエンティティA01~Annが構成され、エンティティA1~Anの下位には、さらに、エンティティB01~Bnk、さらに、その下位にエンティティC1~Cnqが設定されている。各エンティティは、図29B、図29Cに示す如く、複数段のノード、リーフによって構成されるツリー形状を持つ。

例えばエンティティBnkの構成は、(b)に示すように、サブルート281

1を頂点ノードとして、末端ノード2812に至るまでの複数ノードを有する。このエンティティは識別子Bnkを持ち、エンティティBnk内のノードに対応するノードキー管理をエンティティBnk独自に実行することにより、末端ノード2812を頂点として設定される下位（子）エンティティの管理を実行する。また、一方、エンティティBnkは、サブルート2811を末端ノードとして持つ上位（親）エンティティAnnの管理下にある。

エンティティCn3の構成は、（c）に示すように、サブルート2851を頂点ノードとして、各デバイスである末端ノード2852、この場合はリーフに至るまで複数ノード、リーフを有する。このエンティティは識別子Cn3を持ち、エンティティCn3内のノード、リーフに対応するノードキー、リーフキー管理をエンティティCn3独自に実行することにより、末端ノード2852に対応するリーフ（デバイス）の管理を実行する。また、一方、エンティティCn3は、サブルート2851を末端ノードとして持つ上位（親）エンティティBn2の管理下にある。各エンティティにおけるキー管理とは、例えばキー更新処理、リボーク処理等であるが、これらは後段で詳細に説明する。

最下段エンティティのリーフであるデバイスには、デバイスの属するエンティティのリーフキーから、自己の属するエンティティの頂点ノードであるサブルートノードに至るパスに位置する各ノードのノードキー及びリーフキーが格納される。例えば末端ノード2852のデバイスは、末端ノード（リーフ）2852から、サブルートノード2851までの各キーを格納する。

図30A及び図30Bを用いて、さらにエンティティの構成について説明する。エンティティは様々な段数によって構成されるツリー構造を持つことが可能である。段数、すなわちデプス（depth）は、エンティティで管理する末端ノードに対応する下位（子）エンティティの数、あるいはリーフとしてのデバイス数に応じて設定可能である。

図30Aに示すような上下エンティティ構成を具体化すると、（b）に示す態様となる。ルートエンティティは、ルートキーを持つ最上段のエンティティである。ルートエンティティの末端ノードに複数の下位エンティティとしてエンティティA、B、Cが設定され、さらに、エンティティCの下位エンティティとして

エンティティ D が設定される。エンティティ C 2901 は、その末端ノードの 1 つ以上のノードをリザーブノード 2950 として保持し、自己の管理するエンティティを増加させる場合、さらに複数段のツリー構成を持つエンティティ C' 2902 をリザーブノード 2950 を頂点ノードとして新設することにより、管理末端ノード 2970 を増加させて、管理末端ノードに増加した下位エンティティを追加することができる。

リザーブノードについて、さらに図 31 を用いて説明する。エンティティ A, 3011 は、管理する下位エンティティ B, C, D... を持ち、1 つのリザーブノード 3021 を持つ。エンティティは管理対象の下位エンティティをさらに増加させたい場合、リザーブノード 3021 に、自己管理の下位エンティティ A', 3012 を設定し、下位エンティティ A', 3012 の末端ノードにさらに管理対象の下位エンティティ F, G を設定することができる。自己管理の下位エンティティ A', 3012 も、その末端ノードの少なくとも 1 つをリザーブノード 3022 として設定することにより、さらに下位エンティティ A'' 3013 を設定して、さらに管理エンティティを増加させることができる。下位エンティティ A'', 3013 の末端ノードにも 1 以上のリザーブノードを確保する。このようなリザーブノード保有構成をとることにより、あるエンティティの管理する下位エンティティは、際限なく増加させることが可能となる。なお、リザーブエンティティは、末端ノードの 1 つのみではなく、複数個設定する構成としてもよい。

それぞれのエンティティでは、エンティティ単位で有効化キーブロック (EKB) が構成され、エンティティ単位でのキー更新、リボーク処理を実行することになる。図 31 のように複数のエンティティ A, A', A'' には各エンティティ個々の有効化キーブロック (EKB) が設定されることになるが、これらは、エンティティ A, A', A'' を共通に管理する例えばあるデバイスメーカーが一括して管理することが可能である。

[新規エンティティの登録処理]

次に、新規エンティティの登録処理について説明する。登録処理シーケンスを図 32 に示す。図 32 のシーケンスにしたがって説明する。新たにツリー構成中に追加される新規 (子) エンティティ (N-E_n) は、上位 (親) エンティティ

(P-E_n) に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ (P-E_n) に送付する。

登録要求を受領した上位エンティティ (P-E_n) は、受領した新規 (子) エンティティ (N-E_n) の公開鍵を証明書発行局 (CA: Certificate Authority) に転送し、CAの署名を付加した新規 (子) エンティティ (N-E_n) の公開鍵を受領する。これらの手続きは、上位エンティティ (P-E_n) と新規 (子) エンティティ (N-E_n) との相互認証の手続きとして行われる。

これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ (P-E_n) は、新規 (子) エンティティ (N-E_n) の登録を許可し、新規 (子) エンティティ (N-E_n) のノードキーを新規 (子) エンティティ (N-E_n) に送信する。このノードキーは、上位エンティティ (P-E_n) の末端ノードの1つのノードキーであり、かつ、新規 (子) エンティティ (N-E_n) の頂点ノード、すなわちサブルートキーに対応する。

このノードキー送信が終了すると、新規 (子) エンティティ (N-E_n) は、新規 (子) エンティティ (N-E_n) のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティティ内の有効化キーブロック (EKB) を生成する。1つのエンティティ内の有効化キーブロック (EKB) をサブEKBと呼ぶ。

一方、上位エンティティ (P-E_n) は、新規 (子) エンティティ (N-E_n) の追加により、有効化する末端ノードを追加した上位エンティティ (P-E_n) 内のサブEKBを生成する。

新規 (子) エンティティ (N-E_n) は、新規 (子) エンティティ (N-E_n) 内のノードキー、リーフキーによって構成されるサブEKBを生成すると、これを上位エンティティ (P-E_n) に送信する。

新規 (子) エンティティ (N-E_n) からサブEKBを受信した上位エンティティ (P-E_n) は、受信したサブEKBと、上位エンティティ (P-E_n) の更新したサブEKBとをキー発行センタ (KDC: Key Distribute Center) に送信する。

キー発行センタ（KDC）は、全てのエンティティのサブEKBに基づいて、様々な態様のEKB、すなわち特定のエンティティあるいはデバイスのみが復号可能なEKBを生成することが可能となる。このように復号可能なエンティティあるいはデバイスを設定したEKBを例えばコンテンツプロバイダに提供し、コンテンツプロバイダがEKBに基づいてコンテンツキーを暗号化して、ネットワークを介して、あるいは記録媒体に格納して提供することにより、特定のデバイスでのみ利用可能なコンテンツを提供することが可能となる。

なお、新規エンティティのサブEKBのキー発行センタ（KDC）に対する登録処理は、サブEKBを上位エンティティを介してを順次転送して実行する方法に限るものではなく、上位エンティティを介さずに、新規登録エンティティから直接、キー発行センタ（KDC）に登録する処理を実行する構成としてもよい。

上位エンティティと、上位エンティティに新規追加する下位エンティティとの対応について図33を用いて説明する。上位エンティティの末端ノードの1つ3201を新規追加エンティティの頂点ノードとして、下位エンティティに提供することによって下位エンティティは、上位エンティティの管理下のエンティティとして追加される。上位エンティティの管理下のエンティティとは、後段で詳細に説明するが、下位エンティティのリボーク（排除）処理を上位エンティティが実行できる構成であるという意味を含むものである。

図33に示すように、上位エンティティに新規エンティティが設定されると、上位エンティティのリーフである末端ノードの1つのノード3201と新規追加エンティティの頂点ノード3202とが等しいノードとして設定される。すなわち上位ノードの1つのリーフである1つの末端ノードが、新規追加エンティティのサブルートとして設定される。このように設定されることにより、新規追加エンティティが全体ツリー構成の下で有効化される。

図34A及び図34Bに新規追加エンティティを設定した際に上位エンティティが生成する更新EKBの例を示す。図34A及び図34Bは、図34Aに示す構成、すなわち既に有効に存在する末端ノード（node000）3301と末端ノード（node001）3302があり、ここに新規追加エンティティに新規エンティティ追加末端ノード（node100）3303を付与した際に上位

エンティティが生成するサブEKBの例を示したものである。

サブEKBは、図34Bに示すような構成を持つ。それぞれ有効に存在する末端ノードキーにより暗号化された上位ノードキー、上位ノードキーで暗号化されたさらなる上位ノードキー、…さらに上位に進行してサブルートキーに至る構成となっている。この構成によりサブEKBが生成される。各エンティティは図34Bに示すと同様、有効な末端ノード、あるいはリーフキーにより暗号化された上位ノードキー、上位ノードキーでさらに上位のノードキーを暗号化し、順次上位に深層してサブルートに至る暗号化データによって構成されるEKBを有し、これを管理する。

[エンティティ管理下におけるリボーク処理]

次に、キー配信ツリー構成をエンティティ単位として管理する構成におけるデバイスあるいはエンティティのリボーク（排除）処理について説明する。先の図3，4では、ツリー構成全体の中から特定のデバイスのみ復号可能で、リボークされたデバイスは復号不可能な有効化キーブロック（EKB）を配信する処理について説明した。図3，4で説明したリボーク処理は、ツリー全体の中から特定のリーフであるデバイスをリボークする処理であったが、ツリーのエンティティ管理による構成では、エンティティ毎にリボーク処理が実行可能となる。

図35以下の図を用いてエンティティ管理下のツリー構成におけるリボーク処理について説明する。図35A乃至図35Dは、ツリーを構成するエンティティの内、最下段のエンティティ、すなわち個々のデバイスを管理しているエンティティによるデバイスのリボーク処理を説明する図である。

図35Aは、エンティティ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティティA01～Ann、さらにその下位段にB01～Bnkのエンティティ、さらにその下位段にC1～cnのエンティティが構成されている。最も下のエンティティは、末端ノード（リーフ）が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

ここで、リボーク処理は、各エンティティにおいて独自に実行される。例えば、最下段のエンティティC1～Cnでは、リーフのデバイスのリボーク処理が実行される。図35Bには、最下段のエンティティの1つであるエンティティCn，

3 4 3 0 のツリー構成を示している。エンティティ C n, 3 4 3 0 は、頂点ノード 3 4 3 1 を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

この末端ノードであるリーフ中に、リボーク対象となるデバイス、例えばデバイス 3 4 3 2 があったとすると、エンティティ C n, 3 4 3 0 は、独自に更新したエンティティ C n 内のノードキー、リーフキーによって構成される有効化キーブロック（サブ E K B）を生成する。この有効化キーブロックは、リボークデバイス 3 4 3 2 においては復号できず、他のリーフを構成するデバイスにおいてのみ復号可能な暗号化キーにより構成されるキーブロックである。エンティティ C n の管理者は、これを更新されたサブ E K B として生成する。具体的には、サブルートからリボークデバイス 3 4 3 2 に連なるパスを構成する各ノード 3 4 3 1, 3 4 3 4, 3 4 3 5 のノードキーを更新して、この更新ノードキーをリボークデバイス 3 4 3 2 以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成したブロックを更新サブ E K B とする。この処理は、先の図 3, 4 において説明したリボーク処理構成において、ルートキーを、エンティティの頂点キーであるサブルートキーに置き換えた処理に対応する。

このようにエンティティ C n, 3 4 3 0 がリボーク処理によって更新した有効化キーブロック（サブ E K B）は、上位エンティティに送信される。この場合、上位エンティティはエンティティ B n k, 3 4 2 0 であり、エンティティ C n, 3 4 3 0 の頂点ノード 3 4 3 1 を末端ノードとして有するエンティティである。

エンティティ B n k, 3 4 2 0 は、下位エンティティ C n, 3 4 3 0 から有効化キーブロック（サブ E K B）を受領すると、そのキーブロックに含まれるエンティティ C n k, 3 4 3 0 の頂点ノード 3 4 3 1 に対応するエンティティ B n k, 3 4 2 0 の末端ノード 3 4 3 1 を、下位エンティティ C n, 3 4 3 0 において更新されたキーに設定して、自身のエンティティ B n k, 3 4 2 0 のサブ E K B の更新処理を実行する。図 3 5 C にエンティティ B n k, 3 4 2 0 のツリー構成を示す。エンティティ B n k, 3 4 2 0 において、更新対象となるノードキーは、図 3 5 C のサブルート 3 4 2 1 からリボークデバイスを含むエンティティを構成する末端ノード 3 4 3 1 に至るパス上のノードキーである。すなわち、更新サブ E K B を送信してきたエンティティのノード 3 4 3 1 に連なるパスを構成する各

ノード3421, 3424, 3425のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティティBnk, 3420の新たな更新サブEKBを生成する。

さらに、エンティティBnk, 3420が更新した有効化キーブロック（サブEKB）は、上位エンティティに送信される。この場合、上位エンティティはエンティティAnn, 3410であり、エンティティBnk, 3420の頂点ノード3421を末端ノードとして有するエンティティである。

エンティティAnn, 3410は、下位エンティティBnk, 3420から有効化キーブロック（サブEKB）を受領すると、そのキーブロックに含まれるエンティティBnk, 3420の頂点ノード3421に対応するエンティティAnn, 3410の末端ノード3421を、下位エンティティBnk, 3420において更新されたキーに設定して、自身のエンティティAnn, 3410のサブEKBの更新処理を実行する。図35DにエンティティAnn, 3410のツリー構成を示す。エンティティAnn, 3410において、更新対象となるノードキーは、図35Dのサブルート3411から更新サブEKBを送信してきたエンティティのノード3421に連なるバスを構成する各ノード3411, 3414, 3415のノードキーである。これら各ノードのノードキーを更新してエンティティAnn, 3410の新たな更新サブEKBを生成する。

これらの処理を順次、上位のエンティティにおいて実行し、図30Bで説明したルートエンティティまで実行する。この一連の処理により、デバイスのリポー処理が完結する。なお、それぞれのエンティティにおいて更新されたサブEKBは、最終的にキー発行センタ（KDC）に送信され、保管される。キー発行センタ（KDC）は、全てのエンティティの更新サブEKBに基づいて、様々なEKBを生成する。更新EKBは、リポーされたデバイスでの復号が不可能な暗号化キーブロックとなる。

デバイスのリポー処理のシーケンス図を図36に示す。処理手順を図36のシーケンス図に従って説明する。まず、ツリー構成の最下段にあるデバイス管理エンティティ（D-En）は、デバイス管理エンティティ（D-En）内のリポー対象のリーフを排除するために必要なキー更新を行ない、デバイス管理エン

ティティ (D-E_n) の新たなサブEKB (D) を生成する。更新サブEKB (D) は、上位エンティティに送付される。更新サブEKB (D) を受領した上位 (親) エンティティ (P₁-E_n) は、更新サブEKB (D) の更新頂点ノードに対応した末端ノードキーの更新及び、その末端ノードからサブルートに至るパス上のノードキーを更新した更新サブEKB (P₁) を生成する。これらの処理を順次、上位エンティティにおいて実行して、最終的に更新された全てのサブEKBがキー発行センタ (KDC) に格納され管理される。

図37A及び図37Bにデバイスのリボーク処理によって上位エンティティが更新処理を行なって生成する有効化キープロック (EKB) の例を示す。

図37A及び図37Bは、図37Aに示す構成において、リボークデバイスを含む下位エンティティから更新サブEKBを受信した上位エンティティにおいて生成するEKBの例を説明する図である。リボークデバイスを含む下位エンティティの頂点ノードは、上位エンティティの末端ノード (node 100) 3601に対応する。

上位エンティティは、上位エンティティのサブルートから末端ノード (node 100) 3601までのパスに存在するノードキーを更新して新たな更新サブEKBを生成する。更新サブEKBは、図37Bのようになる。更新されたキーは、下線及び「'」を付して示してある。このように更新された末端ノードからサブルートまでのパス上のノードキーを更新してそのエンティティにおける更新サブEKBとする。

次に、リボークする対象をエンティティとした場合の処理、すなわちエンティティのリボーク処理について説明する。

図38Aは、エンティティ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティティA₀₁~A_n、さらにその下位段にB₀₁~B_{nk}のエンティティ、さらにその下位段にC₁~C_nのエンティティが構成されている。最も下のエンティティは、末端ノード (リーフ) が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

ここで、リボーク処理を、エンティティC_n, 3730に対して実行する場合について説明する。最下段のエンティティC_n, 3730は、図38Bに示すよ

うに頂点ノード 3 4 3 1 を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

エンティティ C_n, 3 7 3 0 をリボークすることにより、エンティティ C_n, 3 7 3 0 に属する全てのデバイスのツリー構造からの一括排除が可能となる。エンティティ C_n, 3 7 3 0 のリボーク処理は、エンティティ C_n, 3 7 3 0 の上位エンティティであるエンティティ B_n k, 3 7 2 0 において実行される。エンティティ B_n k, 3 7 2 0 は、エンティティ C_n, 3 7 3 0 の頂点ノード 3 7 3 1 を末端ノードとして有するエンティティである。

エンティティ B_n k, 3 7 2 0 は、下位エンティティ C_n, 3 7 3 0 のリボークを実行する場合、エンティティ C_n k, 3 7 3 0 の頂点ノード 3 7 3 1 に対応するエンティティ B_n k, 3 7 2 0 の末端ノード 3 7 3 1 を更新し、さらに、そのリボークエンティティ 3 7 3 0 からエンティティ B_n k, 3 7 2 0 のサブルートまでのパス上のノードキーの更新を行ない有効化キーブロックを生成して更新サブ E K B を生成する。更新対象となるノードキーは、図 3 8 C のサブルート 3 7 2 1 からリボークエンティティの頂点ノードを構成する末端ノード 3 7 3 1 に至るパス上のノードキーである。すなわち、ノード 3 7 2 1, 3 7 2 4, 3 7 2 5, 3 7 3 1 のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティティ B_n k, 3 7 2 0 の新たな更新サブ E K B を生成する。

あるいは、エンティティ B_n k, 3 7 2 0 は、下位エンティティ C_n, 3 7 3 0 のリボークを実行する場合、エンティティ C_n k, 3 7 3 0 の頂点ノード 3 7 3 1 に対応するエンティティ B_n k, 3 7 2 0 の末端ノード 3 7 3 1 は更新せず、そのリボークエンティティ 3 7 3 0 からエンティティ B_n k, 3 7 2 0 のサブルートまでのパス上の末端ノード 3 7 3 1 を除くノードキーの更新を行ない有効化キーブロックを生成して更新サブ E K B を生成してもよい。

さらに、エンティティ B_n k, 3 7 2 0 が更新した有効化キーブロック（サブ E K B）は、上位エンティティに送信される。この場合、上位エンティティはエンティティ A_n n, 3 7 1 0 であり、エンティティ B_n k, 3 7 2 0 の頂点ノード 3 7 2 1 を末端ノードとして有するエンティティである。

エンティティ A_n n, 3 7 1 0 は、下位エンティティ B_n k, 3 7 2 0 から有

効化キーブロック（サブEKB）を受領すると、そのキーブロックに含まれるエンティティBnk，3720の頂点ノード3721に対応するエンティティAnn，3710の末端ノード3721を、下位エンティティBnk，3720において更新されたキーに設定して、自身のエンティティAnn，3710のサブEKBの更新処理を実行する。図38DにエンティティAnn，3710のツリー構成を示す。エンティティAnn，3710において、更新対象となるノードキーは、図38Dのサブルート3711から更新サブEKBを送信してきたエンティティのノード3721に連なるバスを構成する各ノード3711，3714，3715のノードキーである。これら各ノードのノードキーを更新してエンティティAnn，3710の新たな更新サブEKBを生成する。

これらの処理を順次、上位のエンティティにおいて実行し、図30Bで説明したルートエンティティまで実行する。この一連の処理により、エンティティのリボーク処理が完結する。なお、それぞれのエンティティにおいて更新されたサブEKBは、最終的にキー発行センタ（KDC）に送信され、保管される。キー発行センタ（KDC）は、全てのエンティティの更新サブEKBに基づいて、様々なEKBを生成する。更新EKBは、リボークされたエンティティに属するデバイスでの復号が不可能な暗号化キーブロックとなる。

エンティティのリボーク処理のシーケンス図を図39に示す。処理手順を図39のシーケンス図に従って説明する。まず、エンティティをリボークしようとするエンティティ管理エンティティ（E-E_n）は、エンティティ管理エンティティ（E-E_n）内のリボーク対象の末端ノードを排除するために必要なキー更新を行ない、エンティティ管理エンティティ（E-E_n）の新たなサブEKB

（E）を生成する。更新サブEKB（E）は、上位エンティティに送付される。更新サブEKB（E）を受領した上位（親）エンティティ（P1-E_n）は、更新サブEKB（E）の更新頂点ノードに対応した末端ノードキーの更新及び、その末端ノードからサブルートに至るバス上のノードキーを更新した更新サブEKB（P1）を生成する。これらの処理を順次、上位エンティティにおいて実行して、最終的に更新された全てのサブEKBがキー発行センタ（KDC）に格納され管理される。キー発行センタ（KDC）は、全てのエンティティの更新サブE

K Bに基づいて、様々なE K Bを生成する。更新E K Bは、リボークされたエンティティに属するデバイスでの復号が不可能な暗号化キープロックとなる。

図40にリボークされた下位エンティティと、リボークを行なった上位エンティティの対応を説明する図を示す。上位エンティティの末端ノード3901は、エンティティのリボークにより更新され、上位エンティティのツリーにおける末端ノード3901からサブルートまでのパスに存在するノードキーの更新により、新たなサブE K Bが生成される。その結果、リボークされた下位エンティティの頂点ノード3902のノードキーと、上位エンティティの末端ノード3901のノードキーは不一致となる。エンティティのリボーク後にキー発行センタ(K D C)によって生成されるE K Bは、上位エンティティにおいて更新された末端ノード3901のキーに基づいて生成されることになるので、その更新キーを保有しない下位エンティティのリーフに対応するデバイスは、キー発行センタ(K D C)によって生成されるE K Bの復号が不可能になる。

なお、上述の説明では、デバイスを管理する最下段のエンティティのリボーク処理について説明したが、ツリーの中段にあるエンティティ管理エンティティをその上位エンティティがリボークする処理も上記と同様のプロセスによって可能である。中段のエンティティ管理エンティティをリボークすることにより、リボークされたエンティティ管理エンティティの下位に属する全ての複数エンティティ及びデバイスを一括してリボーク可能となる。

このように、エンティティ単位でのリボークを実行することにより、1つ1つのデバイス単位で実行するリボーク処理に比較して簡易なプロセスでのリボーク処理が可能となる。

【エンティティのケイバビリティ管理】

次に、エンティティ単位でのキー配信ツリー構成において、各エンティティの許容するケイバビリティ(Capability)を管理して、ケイバビリティに応じたコンテンツ配信を行う処理構成について説明する。ここでケイバビリティとは、例えば特定の圧縮音声データの復号が可能であるとか、特定の音声再生方式を許容するとか、あるいは特定の画像処理プログラムを処理できる等、デバイスがどのようなコンテンツ、あるいはプログラム等を処理できるデバイスであるか、すなわ

ちデバイスのデータ処理能力の定義情報である。

図41にケイバビリティを定義したエンティティ構成例を示す。キー配信ツリー構成の最頂点にルートノードが位置し、下層に複数のエンティティが接続されて各ノードが2分岐を持つツリー構成である。ここで、例えばエンティティ4001は、音声再生方式A、B、Cのいずれかを許容するケイバビリティを持つエンティティとして定義される。具体的には、例えばある音声圧縮プログラムA、B、又はC方式で圧縮した音楽データを配信した場合に、エンティティ4001以下に構成されたエンティティに属するデバイスは圧縮データを伸長する処理が可能である。

同様にエンティティ4002は音声再生方式B又はC、エンティティ4003は音声再生方式A又はB、エンティティ4004は音声再生方式B、エンティティ4005は音声再生方式Cを処理することが可能なケイバビリティを持つエンティティとして定義される。

一方、エンティティ4021は、画像再生方式p、q、rを許容するエンティティとして定義され、エンティティ4022は方式p、qの画像再生方式、エンティティ4023は方式pの画像再生が可能なケイバビリティを持つエンティティとして定義される。

このような各エンティティのケイバビリティ情報は、キー発行センタ(KDC)において管理される。キー発行センタ(KDC)は、例えばあるコンテンツプロバイダが特定の圧縮プログラムで圧縮した音楽データを様々なデバイスに配信したい場合、その特定の圧縮プログラムを再生可能なデバイスに対してのみ復号可能な有効化キーブロック(EKB)を各エンティティのケイバビリティ情報に基づいて生成することができる。コンテンツを提供するコンテンツプロバイダは、ケイバビリティ情報に基づいて生成した有効化キーブロック(EKB)によって暗号化したコンテンツキーを配信し、そのコンテンツキーで暗号化した圧縮音声データを各デバイスに提供する。この構成により、データの処理が可能なデバイスに対してのみ特定の処理プログラムを確実に提供することが可能となる。

なお、図41では全てのエンティティについてケイバビリティ情報を定義している構成であるが、図41の構成ように全てのエンティティにケイバビリティ情

報を定義することは必ずしも必要ではなく、例えば図42に示すようにデバイスが属する最下段のエンティティについてのみケイバビリティを定義して、最下段のエンティティに属するデバイスのケイバビリティをキー発行センタ(KDC)において管理して、コンテンツプロバイダが望む処理の可能なデバイスにのみ復号可能な有効化キーブロック(EKB)を最下段のエンティティに定義されたケイバビリティ情報に基づいて生成する構成としてもよい。図42では、末端ノードにデバイスが定義されたエンティティ4101=4105におけるケイバビリティが定義され、これらのエンティティについてのケイバビリティをキー発行センタ(KDC)において管理する構成である。例えばエンティティ4101には音声再生については方式B、画像再生については方式rの処理が可能なデバイスが属している。エンティティ4102には音声再生については方式A、画像再生については方式qの処理が可能なデバイスが属している等である。

図43A及び図43Bにキー発行センタ(KDC)において管理するケイバビリティ管理テーブルの構成例を示す。ケイバビリティ管理テーブルは、図43Aのようなデータ構成を持つ。すなわち、各エンティティを識別する識別子としてのエンティティID、そのエンティティに定義されたケイバビリティを示すケイバビリティリスト、このケイバビリティリストは図43Bに示すように、例えば音声データ再生処理方式(A)が処理可能であれば[1]、処理不可能であれば[0]、音声データ再生処理方式(B)が処理可能であれば[1]、処理不可能であれば[0]…等、様々な態様のデータ処理についての可否を1ビットづつ[1]又は[0]を設定して構成されている。なお、このケイバビリティ情報の設定方法はこのような形式に限らず、エンティティの管理デバイスについてのケイバビリティを識別可能であれば他の構成でもよい。

ケイバビリティ管理テーブルには、さらに、各エンティティのサブEKB、あるいはサブEKBが別のデータベースに格納されている場合は、サブEKBの識別情報が格納され、さらに、各エンティティのサブルートノード識別データが格納される。

キー発行センタ(KDC)は、ケイバビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キーブロック

(EKB) を生成する。図 4 4 を用いて、ケイパビリティ情報に基づく有効化キーブロックの生成処理について説明する。

まず、ステップ S 4 3 0 1 において、キー発行センタ (KDC) は、ケイパビリティ管理テーブルから、指定されたケイパビリティを持つエンティティを選択する。具体的には、例えばコンテンツプロバイダが音声データ再生処理方式 A に基づく再生可能なデータを配信したい場合は、図 4 3 A のケイパビリティリストから、例えば音声データ再生処理 (方式 A) の項目が [1] に設定されたエンティティを選択する。

次に、ステップ S 4 3 0 2 において、選択されたエンティティによって構成される選択エンティティ ID のリストを生成する。次に、ステップ S 4 3 0 3 で、選択エンティティ ID によって構成されるツリーに必要なパス (キー配信ツリー構成のパス) を選択する。ステップ S 4 3 0 4 では、選択エンティティ ID のリストに含まれる全てのパス選択が完了したか否かを判定し、完了するまで、ステップ S 4 3 0 3 においてパスを生成する。これは、複数のエンティティが選択された場合に、それぞれのパスを順次選択する処理を意味している。

選択エンティティ ID のリストに含まれる全てのパス選択が完了すると、ステップ S 4 3 0 5 に進み、選択したパスと、選択エンティティによってのみ構成されるキー配信ツリー構造を構築する。

次に、ステップ S 4 3 0 6 において、ステップ S 4 3 0 5 で生成したツリー構造のノードキーの更新処理を行ない、更新ノードキーを生成する。さらに、ツリーを構成する選択エンティティのサブ EKB をケイパビリティ管理テーブルから取り出し、サブ EKB と、ステップ S 4 3 0 6 で生成した更新ノードキーとに基づいて選択エンティティのデバイスにおいてのみ復号可能な有効化キーブロック (EKB) を生成する。このようにして生成した有効化キーブロック (EKB) は、特定のケイパビリティを持つデバイスにおいてのみ利用、すなわち復号可能な有効化キーブロック (EKB) となる。この有効化キーブロック (EKB) で例えばコンテンツキーを暗号化して、そのコンテンツキーで特定プログラムに基づいて圧縮したコンテンツを暗号化してデバイスに提供することで、キー発行センタ (KDC) によって選択された特定の処理可能なデバイスにおいてのみコン

テンツが利用される。

このようにキー発行センタ (KDC) は、ケイバビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キーブロック (EKB) を生成する。従って、新たなエンティティが登録される場合には、その新規登録エンティティのケイバビリティを予め取得することが必要となる。このエンティティ新規登録に伴うケイバビリティ通知処理について図 4 5 を用いて説明する。

図 4 5 は、新規エンティティがキー配信ツリー構成に参加する場合のケイバビリティ通知処理シーケンスを示した図である。

新たにツリー構成中に追加される新規 (子) エンティティ ($N-E_n$) は、上位 (親) エンティティ ($P-E_n$) に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ ($P-E_n$) に送付する。

登録要求を受領した上位エンティティ ($P-E_n$) は、受領した新規 (子) エンティティ ($N-E_n$) の公開鍵を証明書発行局 (CA: Certificate Authority) に転送し、CA の署名を付加した新規 (子) エンティティ ($N-E_n$) の公開鍵を受領する。これらの手続きは、上位エンティティ ($P-E_n$) と新規 (子) エンティティ ($N-E_n$) との相互認証の手続きとして行われる。

これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ ($P-E_n$) は、新規 (子) エンティティ ($N-E_n$) の登録を許可し、新規 (子) エンティティ ($N-E_n$) のノードキーを新規 (子) エンティティ ($N-E_n$) に送信する。このノードキーは、上位エンティティ ($P-E_n$) の末端ノードの 1 つのノードキーであり、かつ、新規 (子) エンティティ ($N-E_n$) の頂点ノード、すなわちサブルートキーに対応する。

このノードキー送信が終了すると、新規 (子) エンティティ ($N-E_n$) は、新規 (子) エンティティ ($N-E_n$) のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティティ内の有効化キーブロック (サブ EKB) を生成する。一方、上位エンティティ ($P-E_n$) も、新規 (子) エンティティ ($N-E_n$)

の追加により、有効化する末端ノードを追加した上位エンティティ（ $P-E_n$ ）内のサブEKBを生成する。

新規（子）エンティティ（ $N-E_n$ ）は、新規（子）エンティティ（ $N-E_n$ ）内のノードキー、リーフキーによって構成されるサブEKBを生成すると、これを上位エンティティ（ $P-E_n$ ）に送信し、さらに、自己のエンティティで管理するデバイスについてのケイバビリティ情報を上位エンティティに通知する。

新規（子）エンティティ（ $N-E_n$ ）からサブEKB及びケイバビリティ情報を受信した上位エンティティ（ $P-E_n$ ）は、受信したサブEKBとケイバビリティ情報と、上位エンティティ（ $P-E_n$ ）の更新したサブEKBとをキー発行センタ（KDC：Key Distribute Center）に送信する。

キー発行センタ（KDC）は、受領したエンティティのサブEKB及びケイバビリティ情報とを図43A及び図43Bで説明したケイバビリティ管理テーブルに登録し、ケイバビリティ管理テーブルを更新する。キー発行センタ（KDC）は、更新したケイバビリティ管理テーブルに基づいて、様々な態様のEKB、すなわち特定のケイバビリティを持つエンティティあるいはデバイスのみが復号可能なEKBを生成することが可能となる。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

以上、説明したように、本発明の情報処理システム及び方法によれば、コンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等の暗号化処理キーブロックとして適用可能な有効化キーブロック（EKB）の生成において、階層的鍵配信ツリーを配信デバイスに応じて再構築して、再構築した簡略ツリーに含まれるノード、リーフに基づいて有効化キーブロック（EKB）を

生成する構成としたので、有効化キープブロック（E K B）の大幅なデータ量削減が実現される。

また、本発明の情報処理システム及び方法によれば、簡略化した再構築階層ツリーに基づく有効化キープブロック（E K B）を構成し、さらに、E K B中の暗号化キーデータの位置識別子としてのタグに暗号化キーデータの有無を判別するデータを含ませた構成としたので、E K Bの大幅なデータ量削減が実現されるとともに、E K Bを受領したデバイスでのタグを用いた暗号化キーデータの抽出が容易となり、デバイスでのE K B復号処理が効率的になる。

請求の範囲

1. 1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、

個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、

前記デバイスに提供される暗号化メッセージデータは、前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーを、該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含む有効化キーブロック（EKB）の復号処理によって得られる前記更新ノードキーによって暗号化されたデータ構成であり、

前記有効化キーブロック（EKB）は、前記暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む構成であることを特徴とする情報処理システム。

2. 前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化したデータであり、

前記タグ部に格納される位置識別データは、前記有効化キーブロック（EKB）に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右ノード又はリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする請求の範囲第1項に記載の情報処理システム。

3. 前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、該有効化キーブロック（EKB）を復号可能な末端ノード又はリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略するこ

とにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キーブロック (E K B) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

4. 前記有効化キーブロック (E K B) に含まれる前記暗号化キーデータは、該有効化キーブロック (E K B) を復号可能な末端ノード又はリーフを最下段とした簡略化した 2 分岐型ツリーを構成するバスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キーブロック (E K B) に格納された 1 以上の暗号化キーデータ各々のノード位置の下位の左右ノード又はリーフ位置の暗号化キーデータの有無を示すタグと、該タグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

5. 前記再構築階層ツリーは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して構成されるツリーであることを特徴とする請求の範囲第 4 項に記載の情報処理システム。

6. 前記有効化キーブロック (E K B) に含まれる前記暗号化キーデータは、該有効化キーブロック (E K B) を復号可能な末端ノード又はリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノード又はリーフと、該多分岐型ツリーの頂点とを直接接続するバスを選択して不要ノードを省略することにより再構築される再構築階層ツリーの頂点ノード及び末端ノード又はリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キーブロック (E K B) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

7. 前記再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノード又はリーフとを直接、接続した 3 以

上の分岐を持つツリーであることを特徴とする請求の範囲第 6 項に記載の情報処理システム。

8. 前記デバイスにおける前記暗号処理手段は、前記有効化キープブロック (EKB) の前記タグ部のデータにより、前記暗号化キーデータを順次抽出して、復号処理を実行し、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

9. 前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

10. 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

11. 前記メッセージデータは、コンテンツのインテグリティ・チェック値 (ICV) 生成キーであることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

12. 前記メッセージデータは、プログラムコードであることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

13. 1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理方法であり、

複数の異なるデバイスをリーフとした階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーを、該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含むデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キープブロック (EKB) を生成する有効化キープブロック (EKB) 生成ステップと、

前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップとを有する情報処理方法。

14. 前記情報処理方法は、さらに、

前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップを有する請求の範囲第13項に記載の情報処理方法。

15. 前記有効化キーブロック (EKB) 生成ステップは、

前記階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化して前記暗号化キーデータを生成するステップと、

前記有効化キーブロック (EKB) に格納される1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノード又はリーフ位置の暗号化キーデータの有無を示すタグを生成して前記タグ部に格納するステップとを含むことを特徴とする請求の範囲第13項に記載の情報処理方法。

16. 前記有効化キーブロック (EKB) 生成ステップは、

該有効化キーブロック (EKB) を復号可能な末端ノード又はリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、

前記再構築階層ツリーの構成ノード又はリーフに対応するキーのみに基づいて有効化キーブロック (EKB) を生成するステップと、

前記有効化キーブロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップとを含むことを特徴とする請求の範囲第13項に記載の情報処理方法。

17. 前記再構築階層ツリーを生成するステップは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して実行されるツリー生成処理であることを特徴とする請求の範囲第16項に記載の情報処理方法。

18. 前記有効化キーブロック (EKB) 生成ステップは、

該有効化キーブロック (EKB) を復号可能な末端ノード又はリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノード又はリーフと、該多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーを生成するステップと、

前記有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップとを含むことを特徴とする請求の範囲第13項に記載の情報処理方法。

19．前記再構築階層ツリーの生成ステップにおいて生成する再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノード又はリーフとを直接、接続した3以上の分岐を持つツリーとして生成することを特徴とする請求の範囲第18項に記載の情報処理方法。

20．前記復号処理ステップは、

前記有効化キーブロック（EKB）の前記タグ部に格納された位置識別データに基づいて前記データ部に格納された暗号化キーデータを順次抽出して順次復号処理を実行することにより前記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含むことを特徴とする請求の範囲第14項に記載の情報処理方法。

21．前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求の範囲第13項に記載の情報処理方法。

22．前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第13項に記載の情報処理方法。

23．前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求の範囲第13項に記載の情報処理方法。

24．前記メッセージデータは、プログラムコードであることを特徴とする請求の範囲第13項に記載の情報処理方法。

25．データを格納した情報記録媒体であり、

複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーを、

該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（EKB）と、

前記更新ノードキーによって暗号化したメッセージデータとを格納した情報記録媒体。

26. 前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキー又は下位リーフキーを用いて暗号化したデータであり、

前記タグ部に格納される位置識別データは、前記有効化キーブロック（EKB）に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノード又はリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする請求の範囲第25項に記載の情報記録媒体。

27. 前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、該有効化キーブロック（EKB）を復号可能な末端ノード又はリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノード又はリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第25項に記載の情報記録媒体。

28. 複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーを、該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）の生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

前記コンピュータ・プログラムは、

該有効化キーブロック（EKB）を復号可能な末端ノード又はリーフを最下段

とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、

前記再構築階層ツリーの構成ノード又はリーフに対応するキーのみに基づいて有効化キーブロック (EKB) を生成するステップと、

前記有効化キーブロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップとを含むことを特徴とするプログラム提供媒体。

29. 複数の異なるデバイスをリーフとした階層ツリー構造における固有のノードキーとリーフキーのキーセットを保持する記憶手段と、

配信される暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理手段を有し、

前記提供される暗号化メッセージデータは、有効化キーブロック (EKB) の前記復号処理手段の復号処理によって得られる更新ノードキーによって暗号化されたデータ構成であり、

前記有効化キーブロック (EKB) は、

前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフキーによって構成されるグループ内のノードキーの少なくともいずれかを更新した前記更新ノードキーを、該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータによって構成されるデータ部と、

該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む構成であることを特徴とする情報処理装置。

30. 前記有効化キーブロック (EKB) に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化したデータであり、

前記タグ部に格納される位置識別データは、前記有効化キーブロック (EKB) に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする請求の範囲第29項に記載の情報処理装置。

31. 前記有効化キープブロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープブロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キープブロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第29項に記載の情報処理装置。

32. 前記有効化キープブロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープブロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キープブロック (EKB) に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグと、該タグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求の範囲第29項に記載の情報処理装置。

33. 前記復号処理手段は、

前記有効化キープブロック (EKB) の前記タグ部のデータにより、前記暗号化キーデータを順次抽出して、復号処理を実行し、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求の範囲第29項に記載の情報処理装置。

34. 配信される暗号化メッセージデータを復号処理する情報処理方法であって、

階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーを、上記グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含む有効化キープブロック (EKB) より、前記暗号化キーデータを取得する暗号化キーデータ取得ステップと、

取得された前記暗号化キーデータを復号することにより上記更新ノードキーを得る更新ノードキー取得ステップとを含み、

前記有効化キープブロック（E K B）は、前記暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む構成であることを特徴とする情報処理方法。

35．前記暗号化キーデータ取得ステップでは、

前記有効化キープブロック（E K B）の前記タグ部に格納された位置識別データに基づいて前記データ部に格納された暗号化キーデータを順次抽出するようになり、

前記更新ノードキー取得ステップでは、取得された上記暗号化キーデータを順次復号処理を実行することにより前記更新ノードキーを取得するようになり、

前記更新ノードキーにより前記暗号化メッセージデータの復号を実行する復号処理ステップを更に有することを特徴とする請求の範囲第34項に記載の情報処理方法。

36．前記復号処理ステップでは、

前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットを保有し、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行するようになり、

37．上記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求の範囲第34項に記載の情報処理方法。

38．上記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第34項に記載の情報処理方法。

39．上記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求の範囲第34項に記載の情報処理方法。

1/45

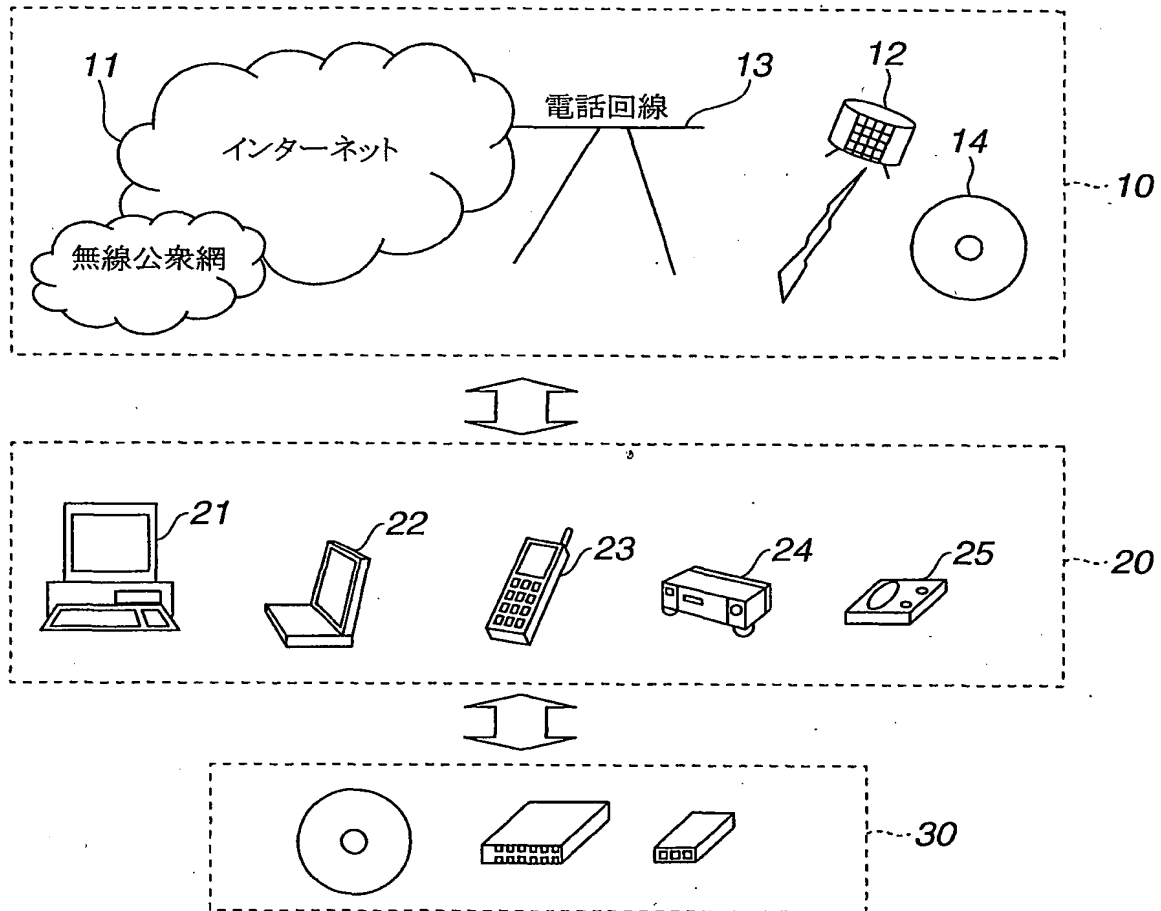


FIG.1

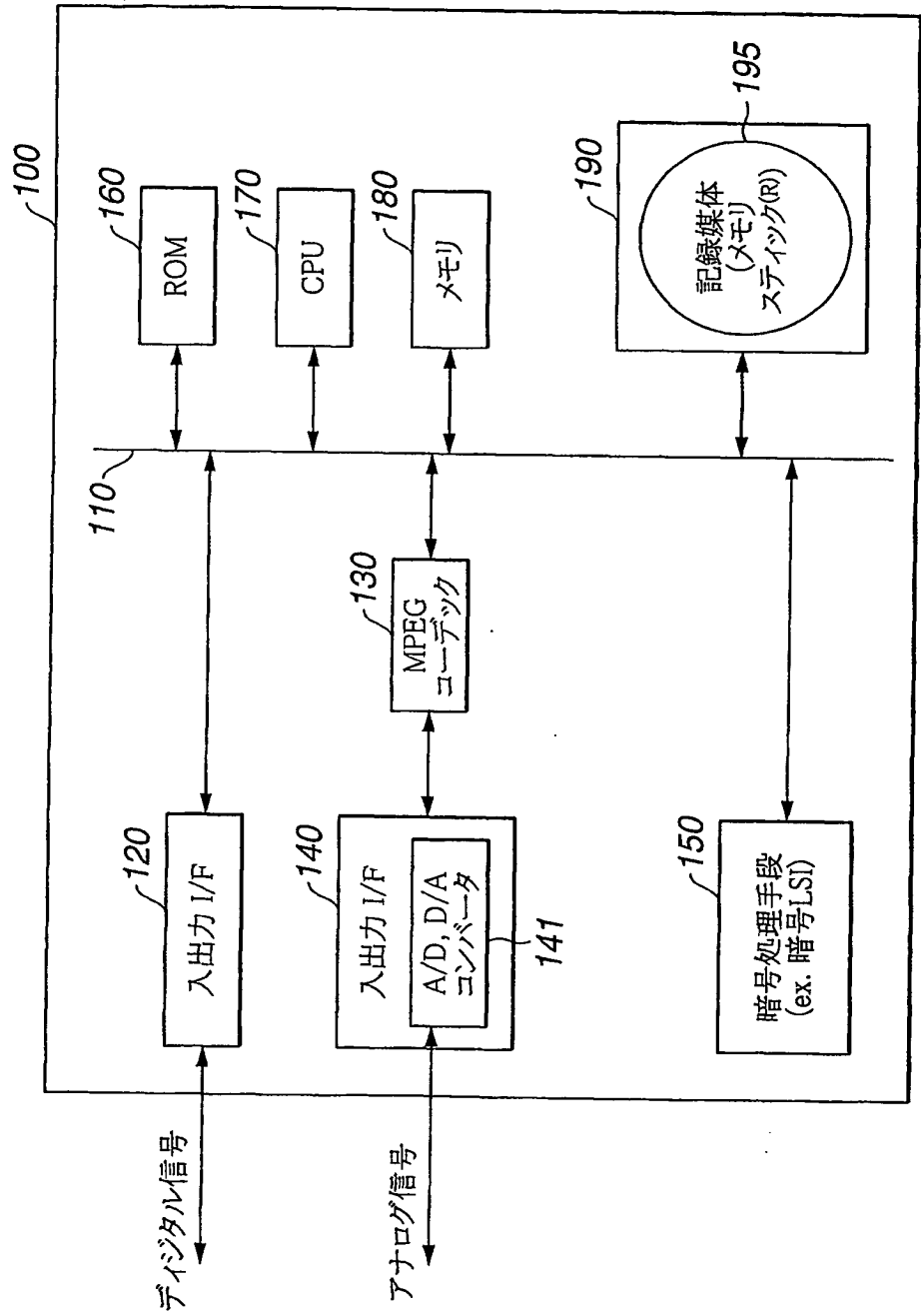


FIG.2

3/45

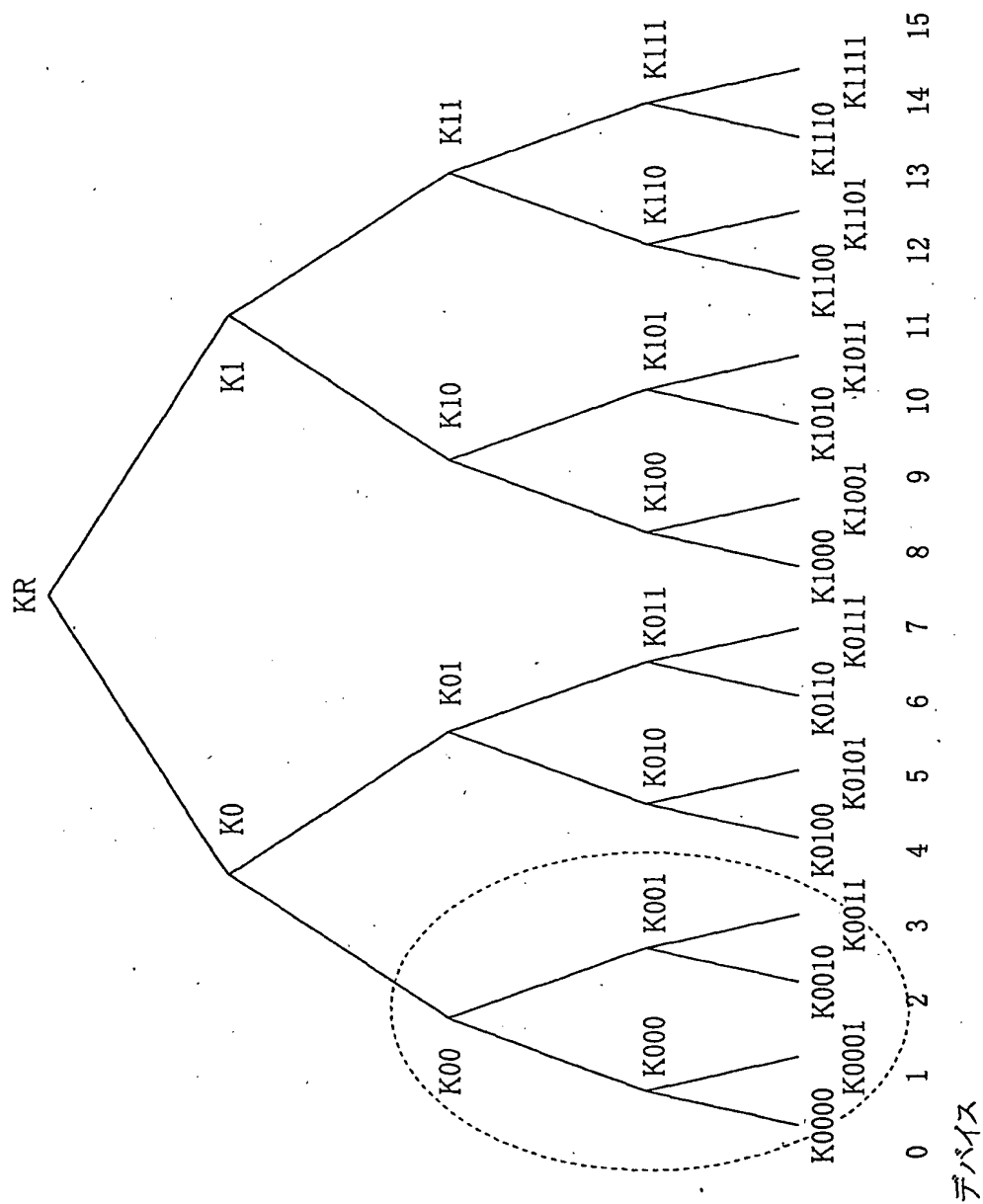


FIG.3

4/45

バージョン (Version) : t	
インデックス	暗号化キー
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG.4A

バージョン (Version) : t	
インデックス	暗号化キー
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG.4B

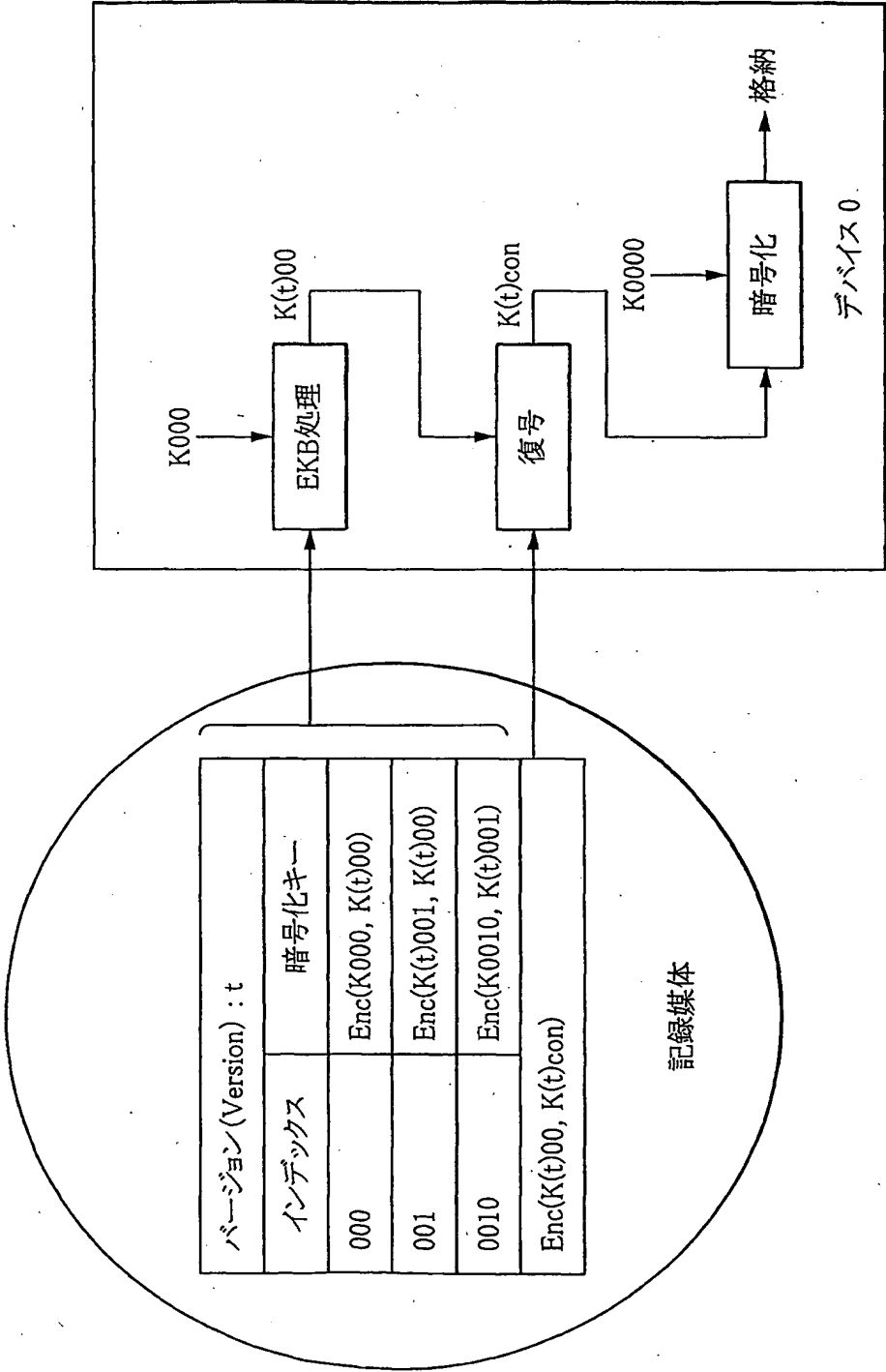


FIG.5

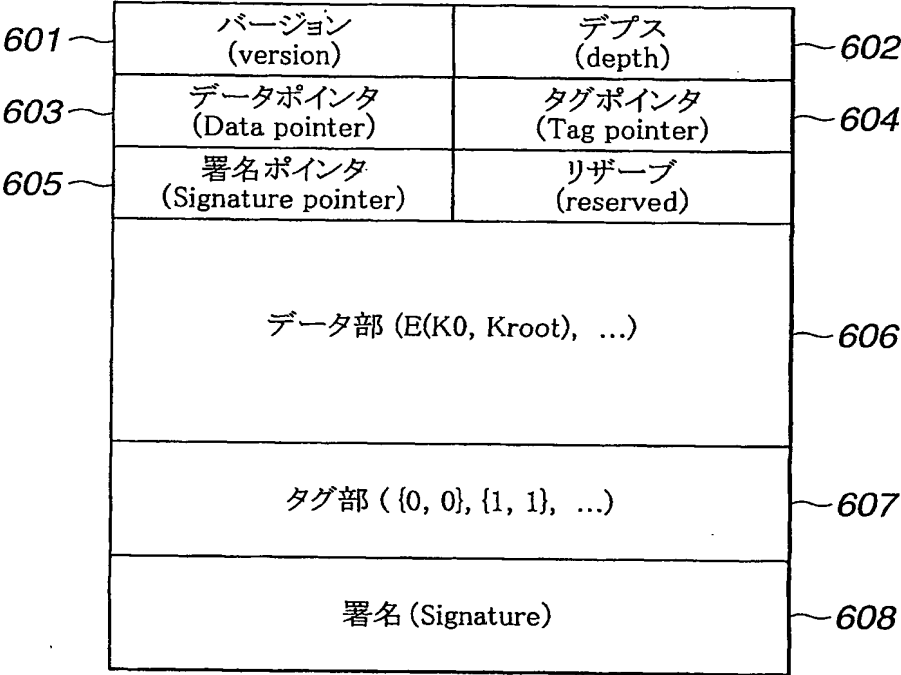


FIG.6

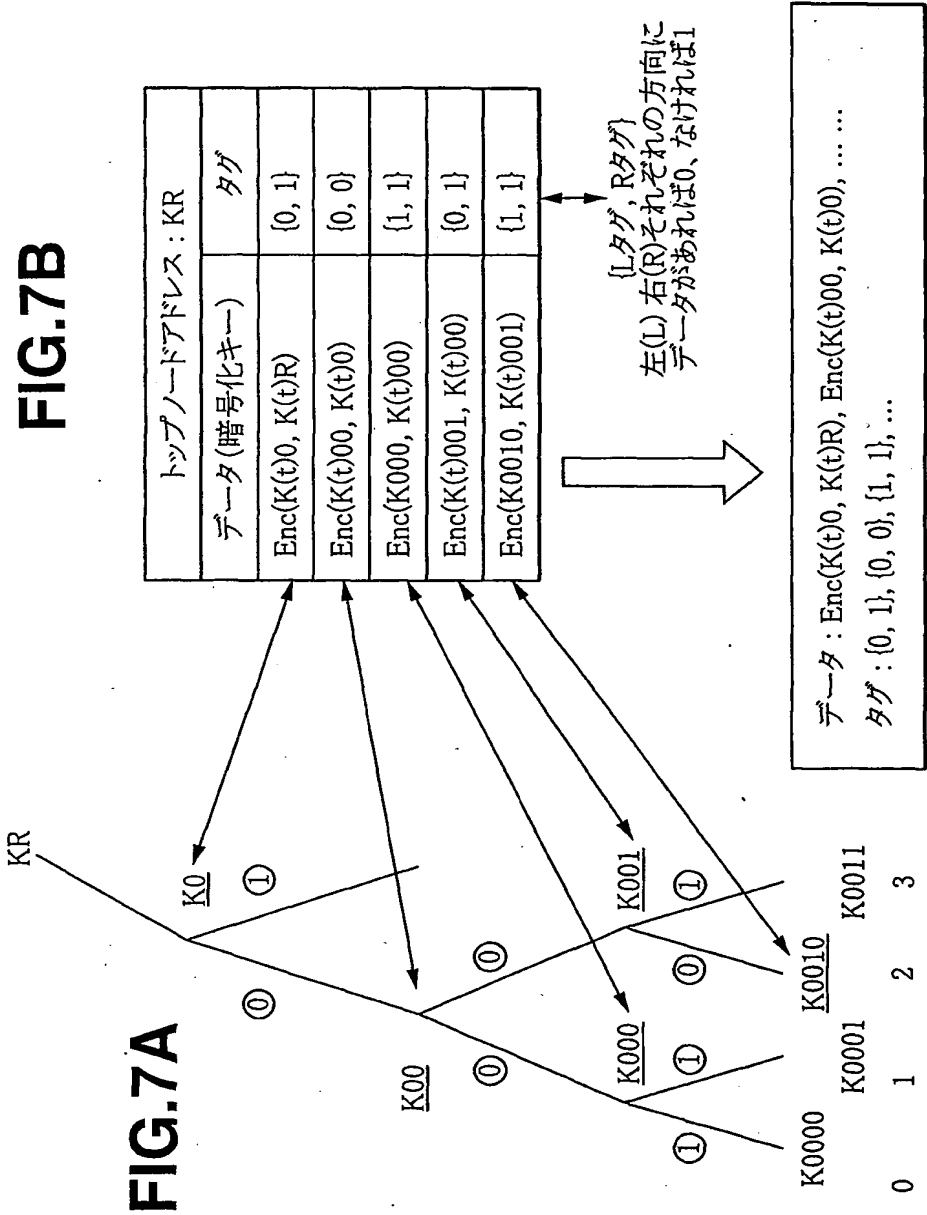


FIG.8A

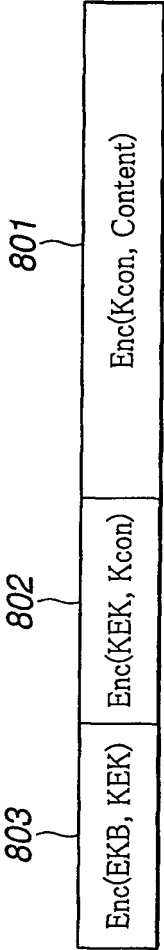
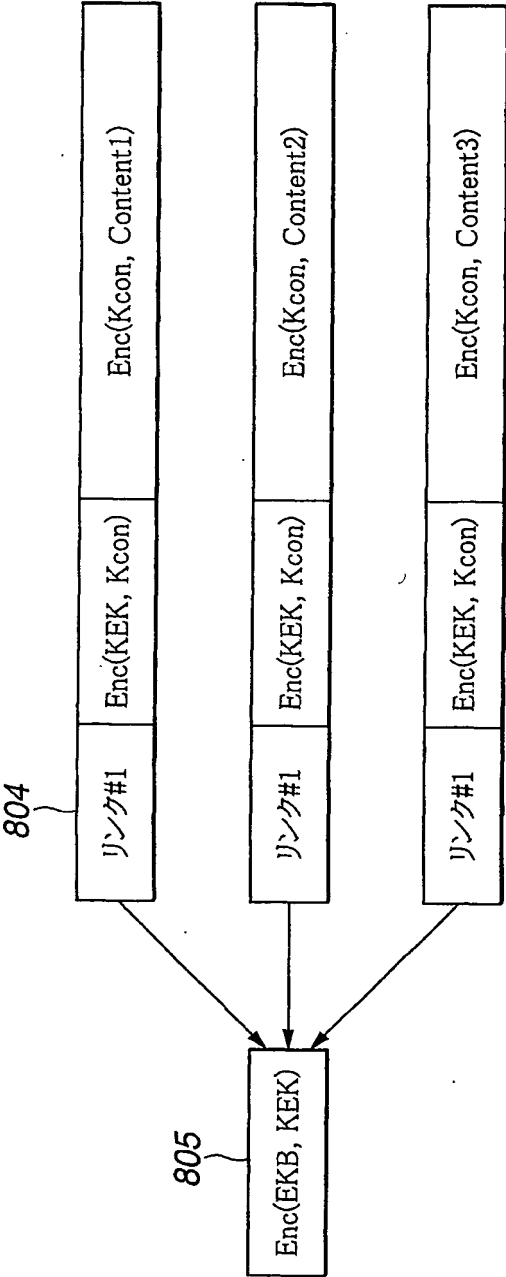


FIG.8B



9/45

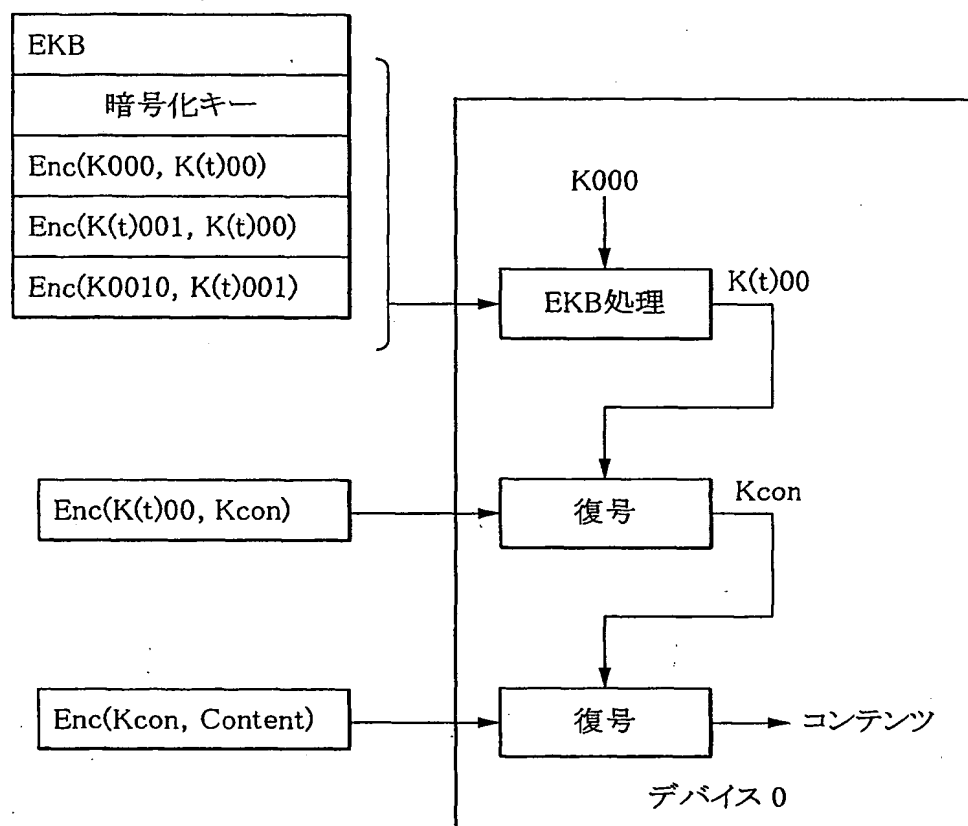


FIG.9

10/45

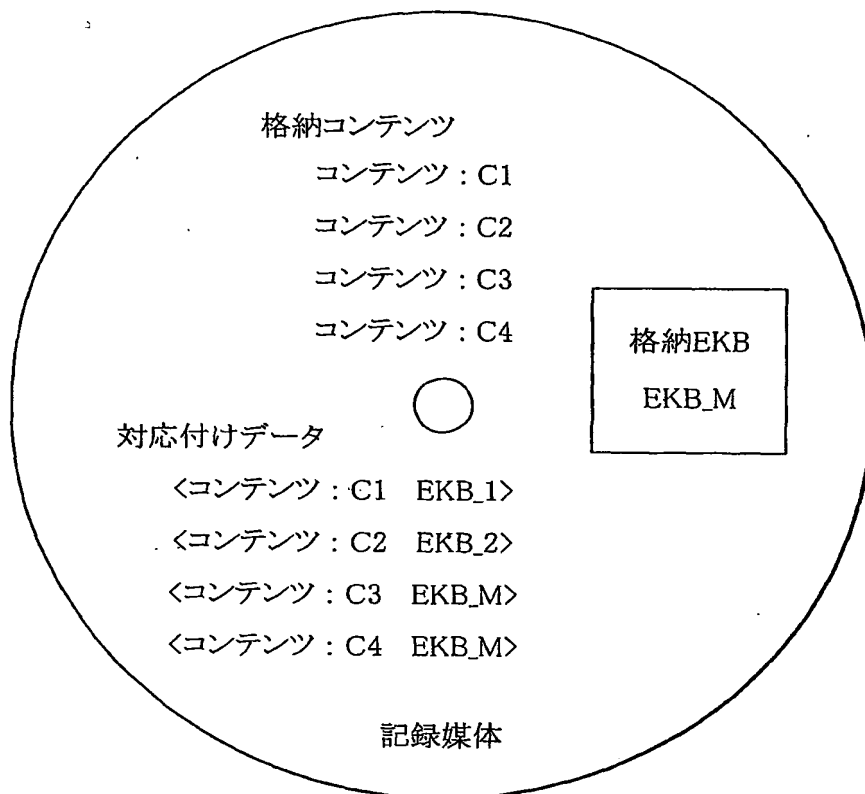


FIG.10

12/45

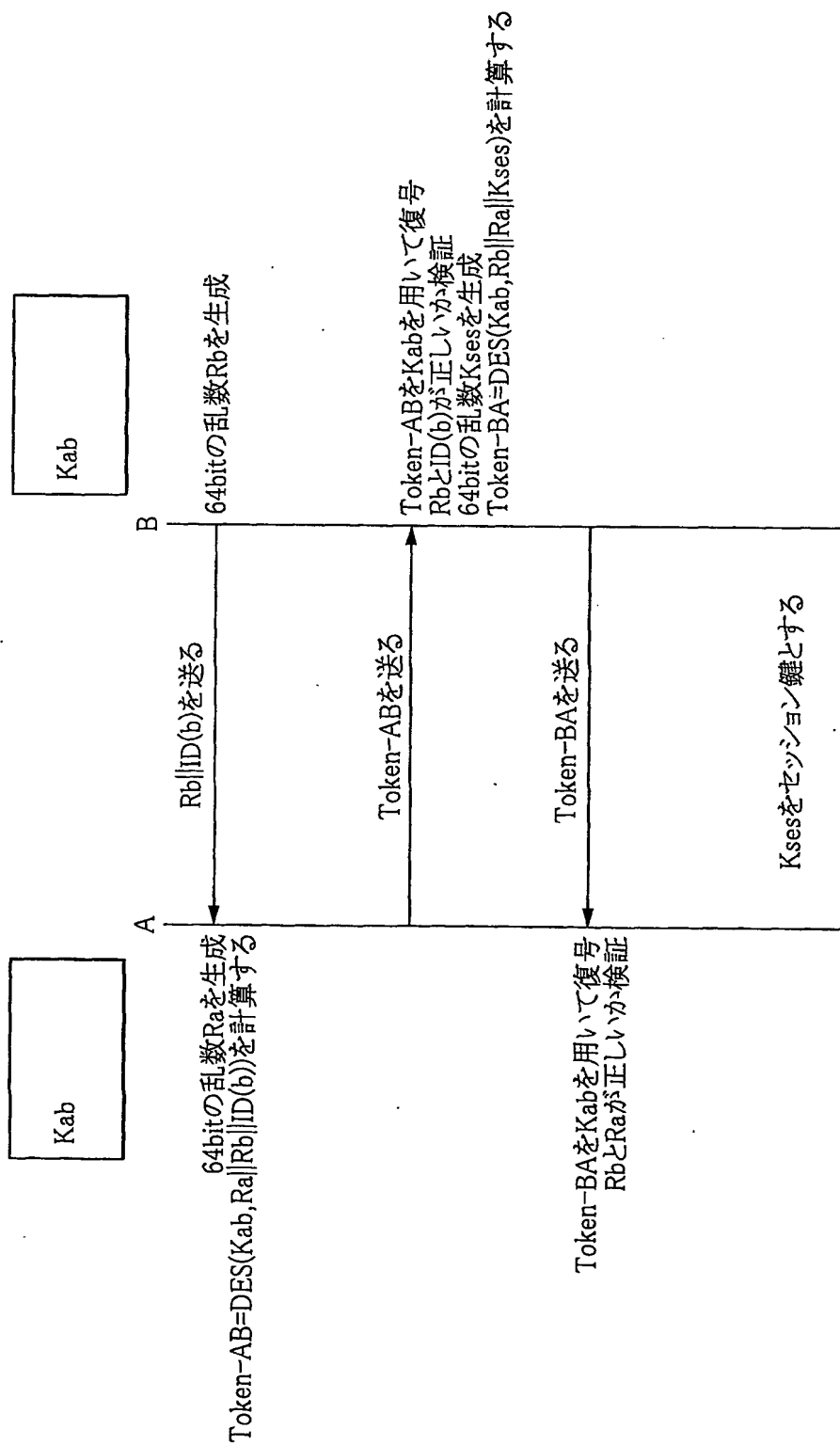


FIG.12

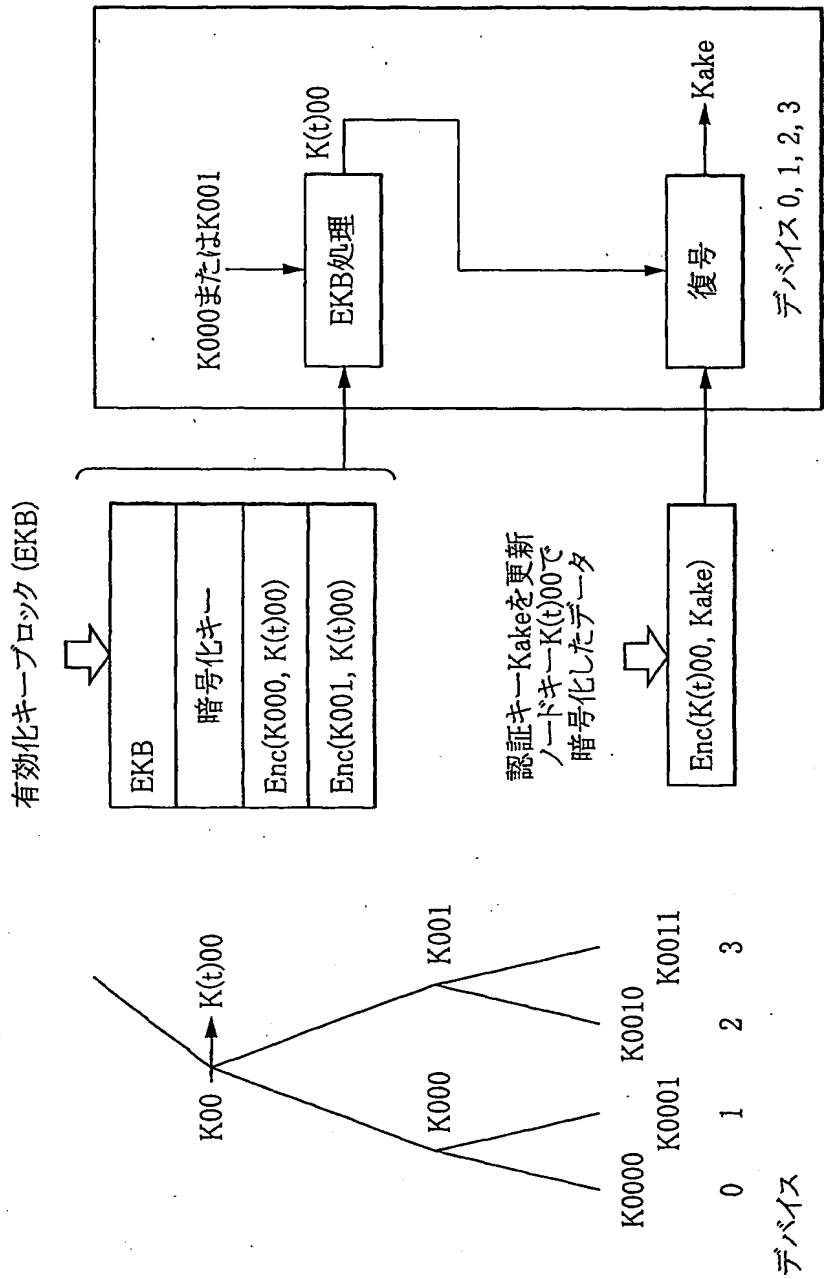


FIG.13

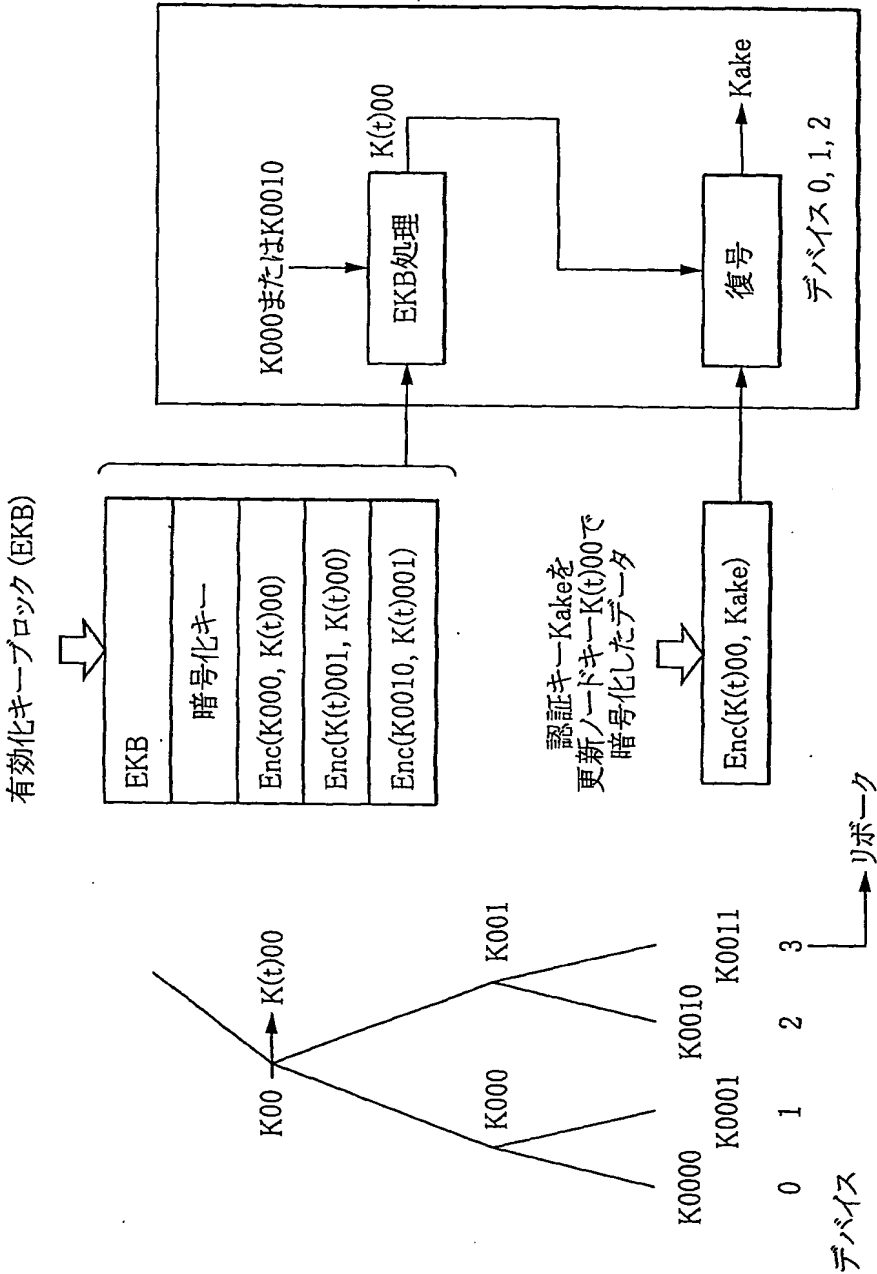


FIG.14

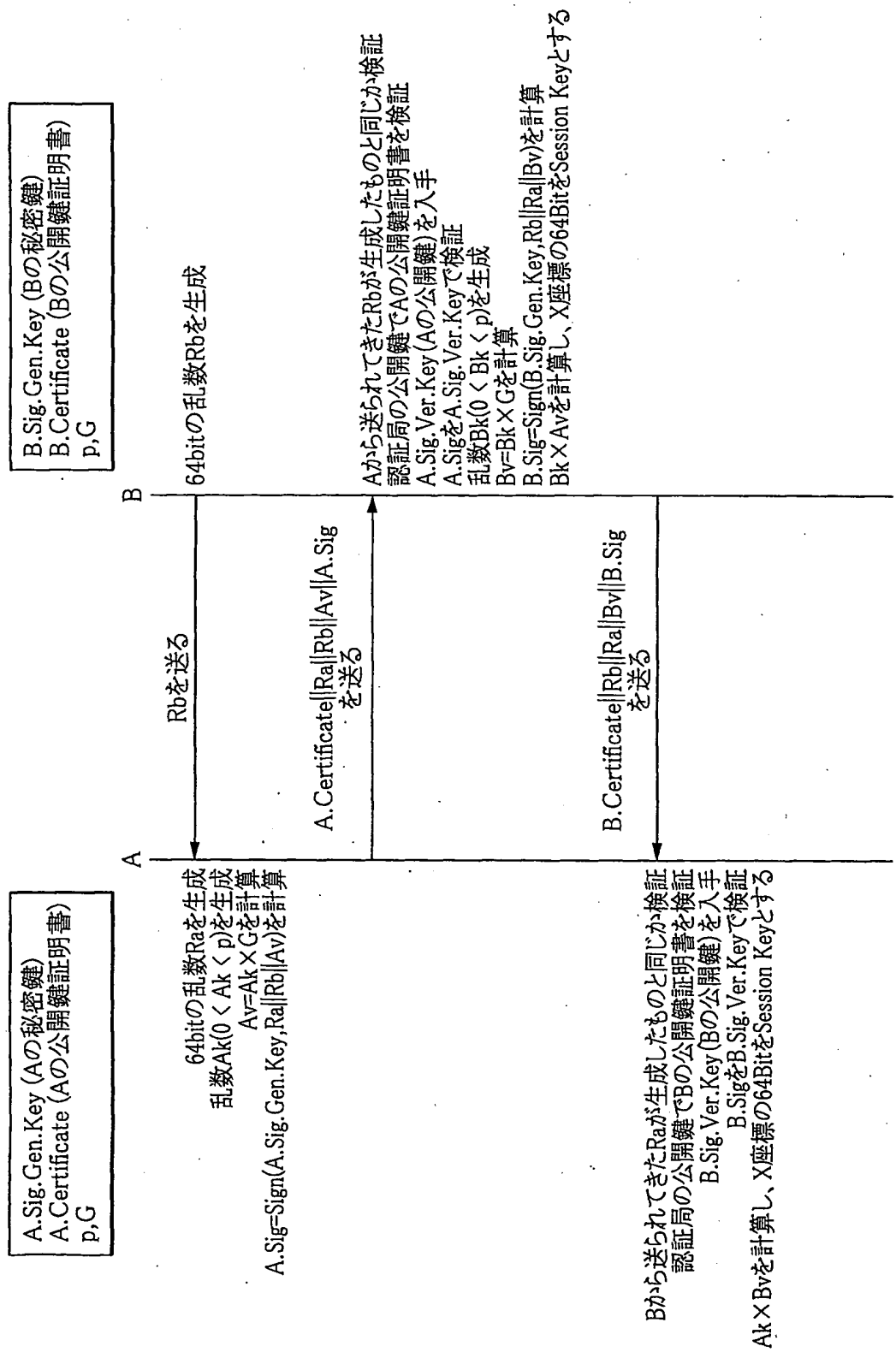


FIG.15

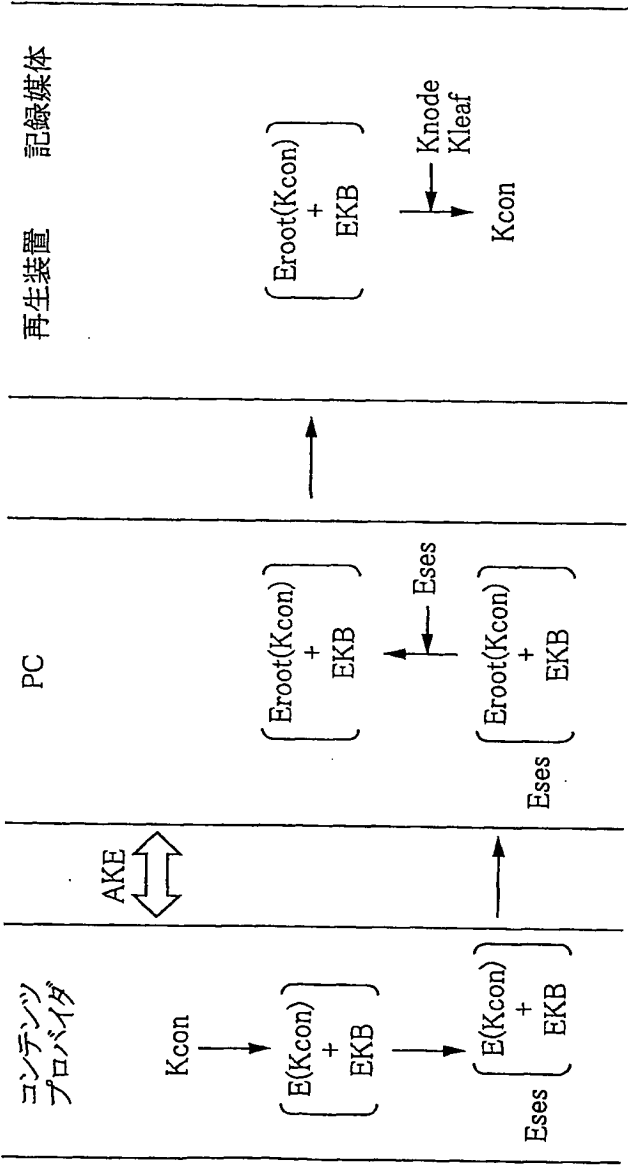


FIG.16

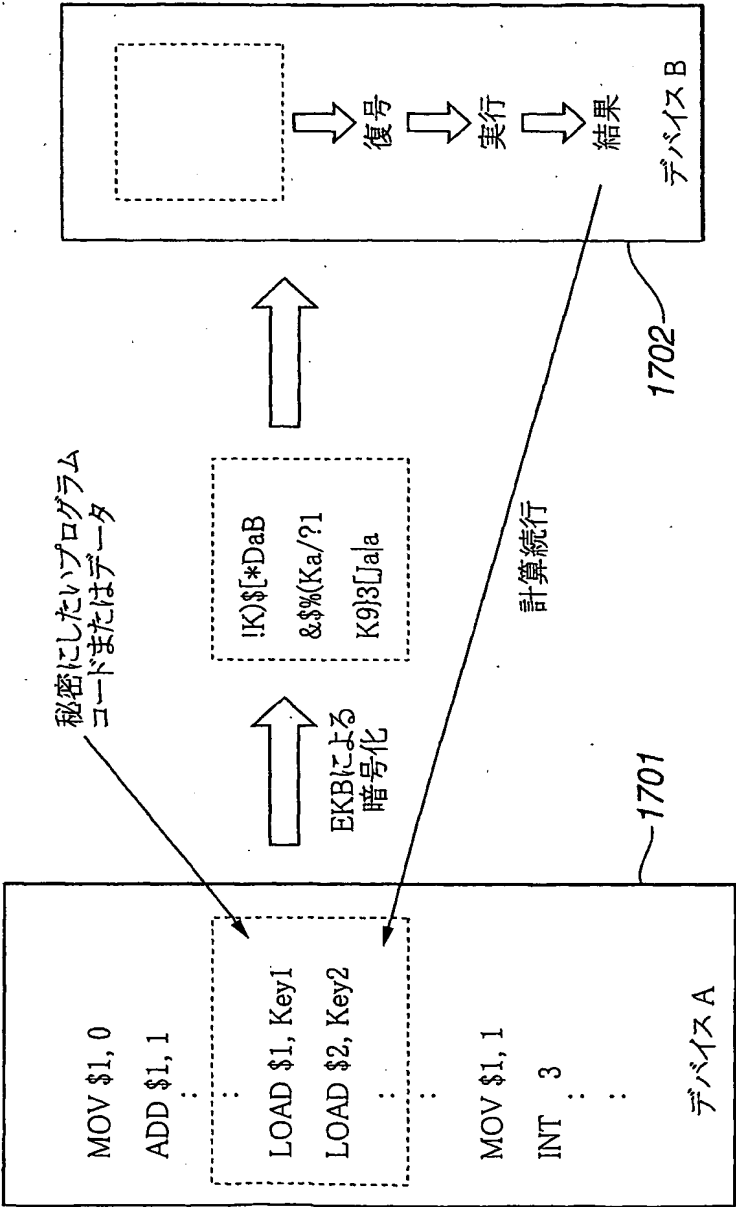


FIG.17

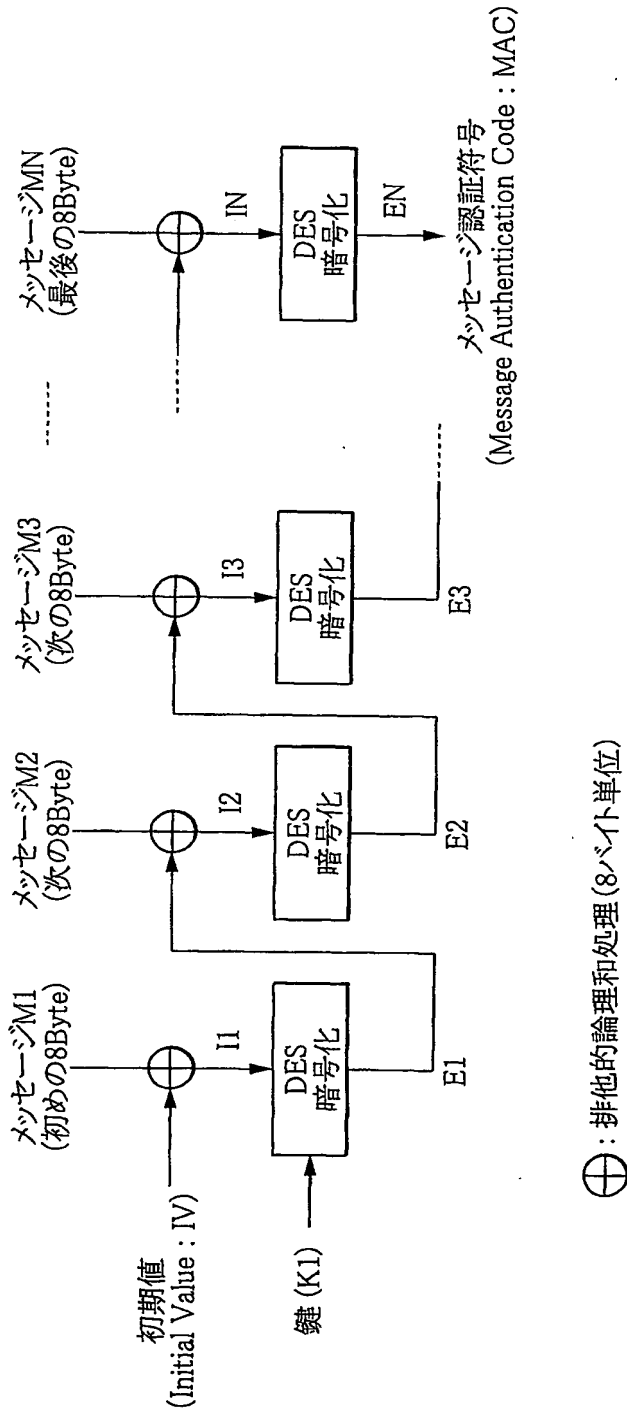


FIG.18

19/45

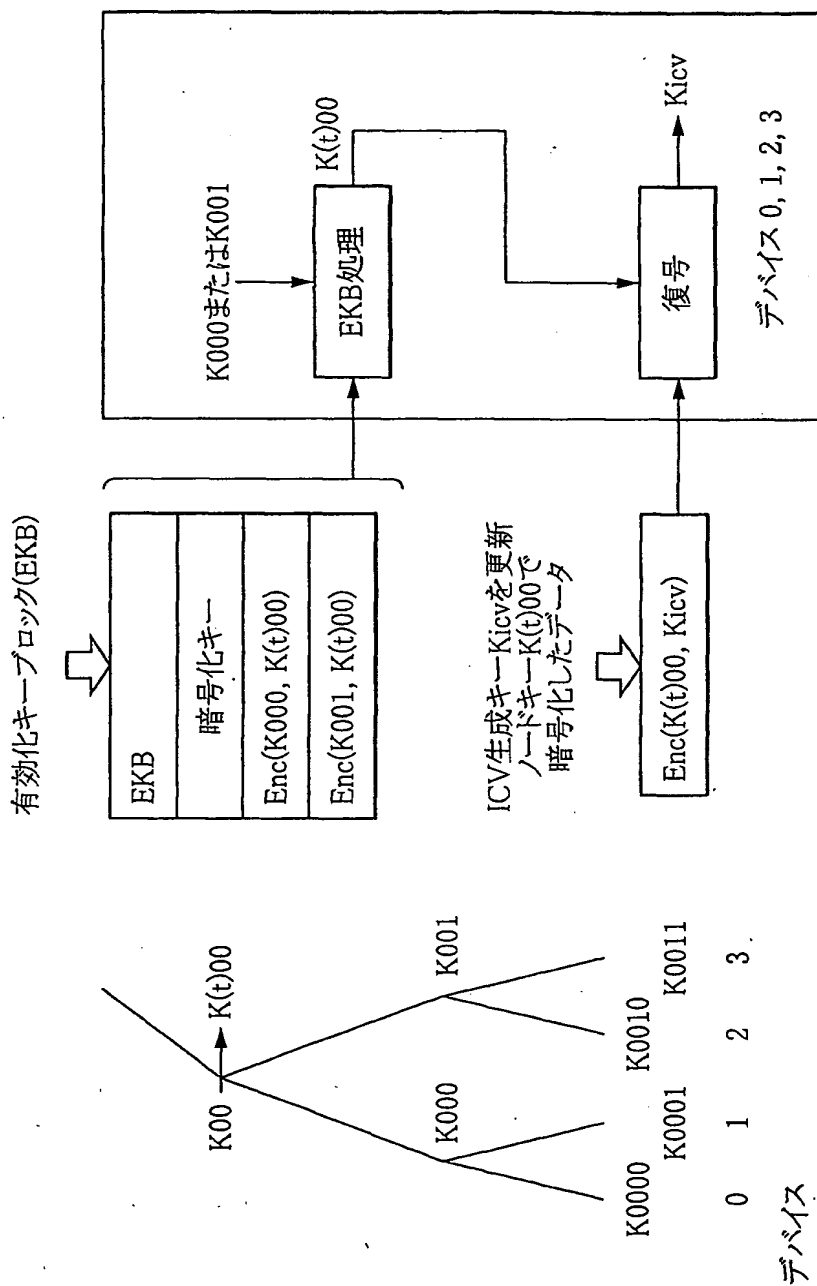


FIG.19

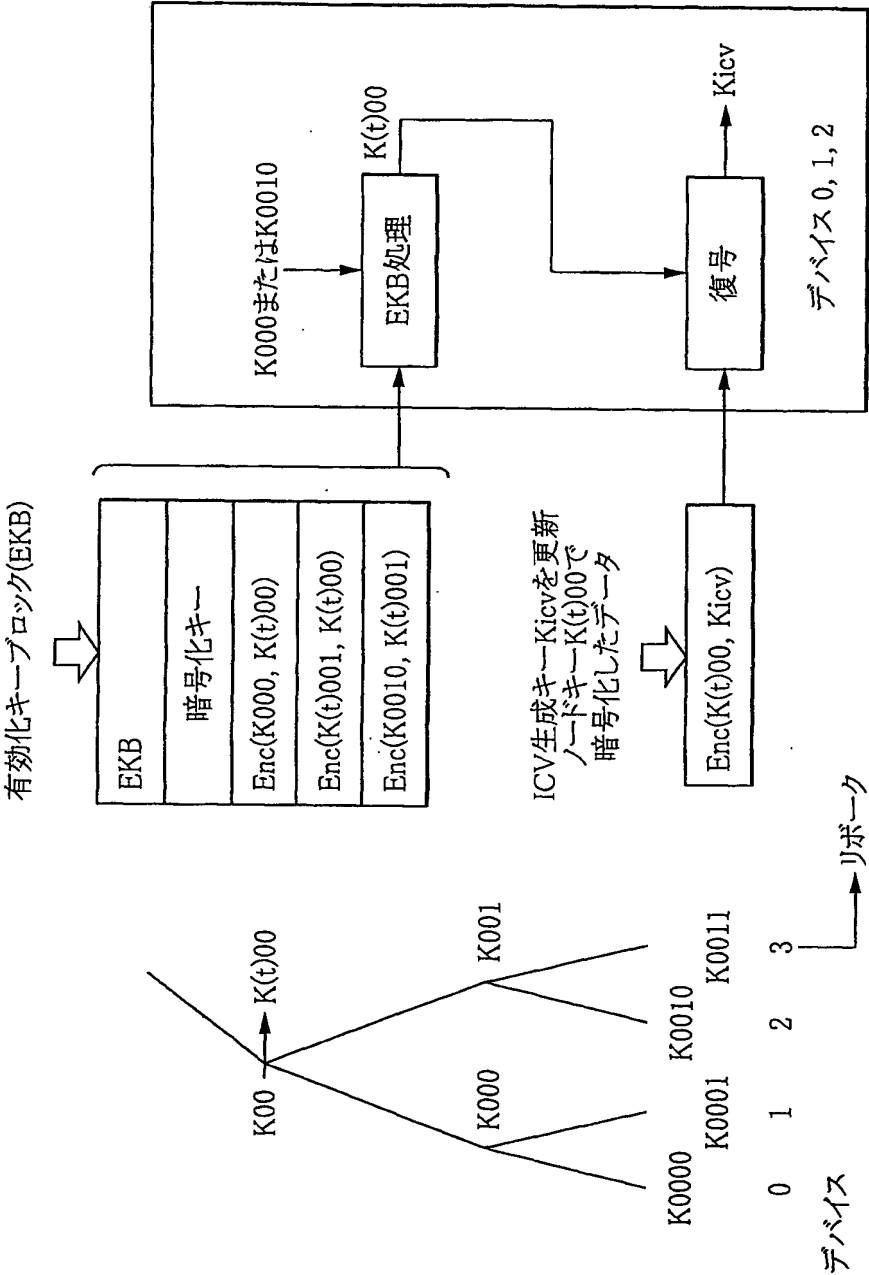


FIG.20

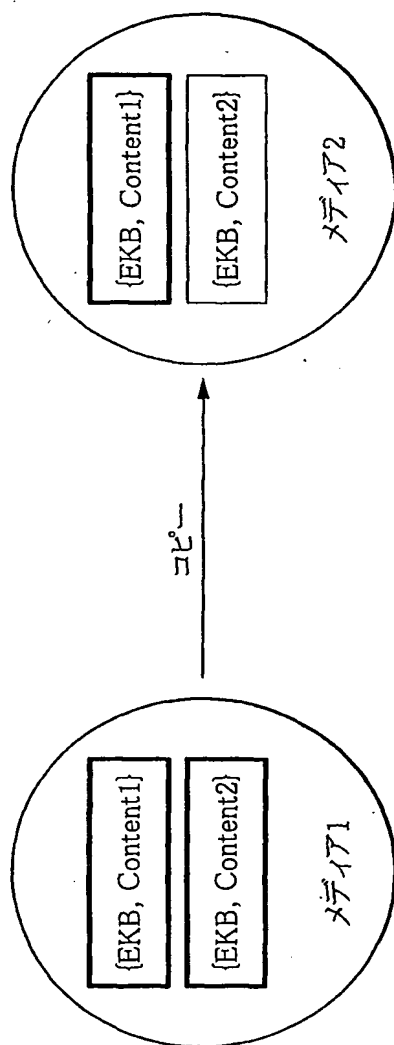


FIG. 21A

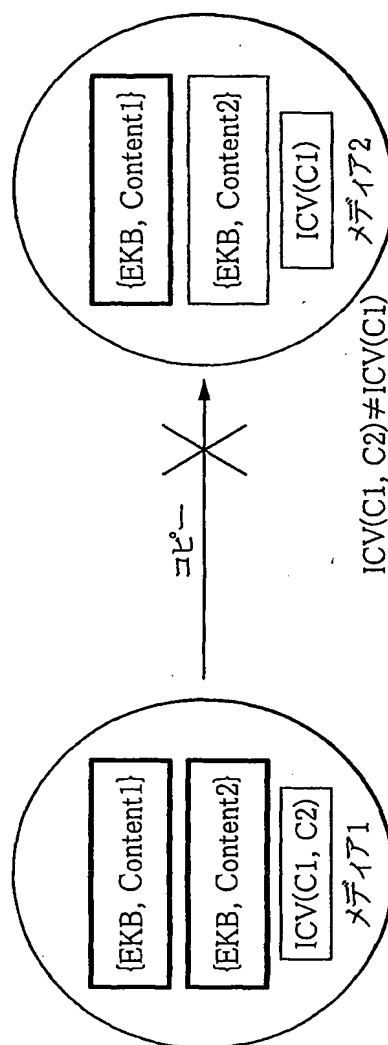


FIG. 21B

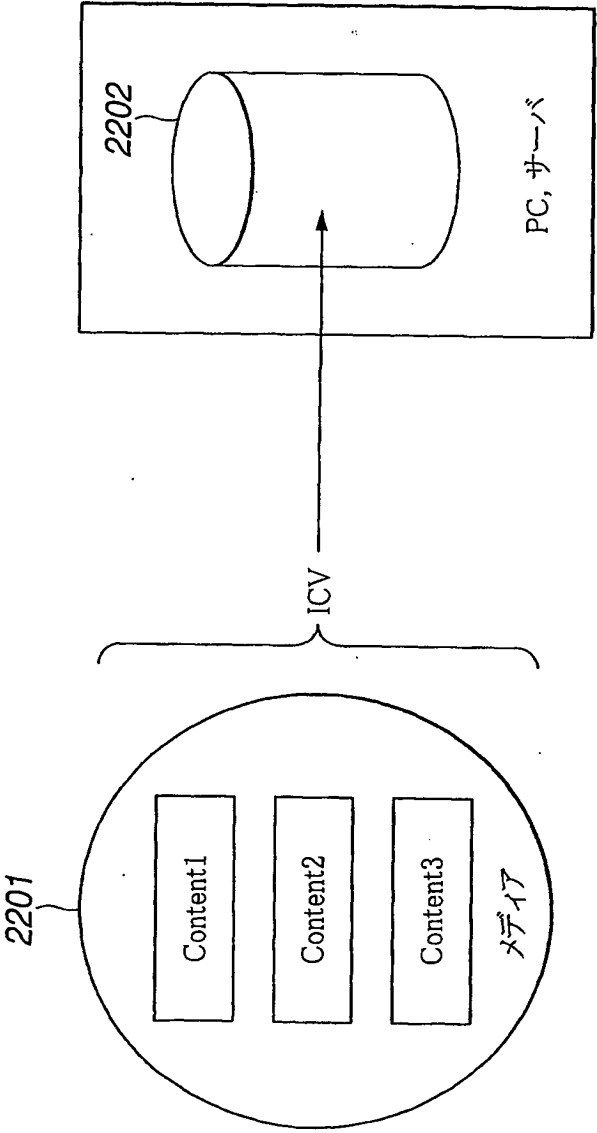


FIG.22

23/45

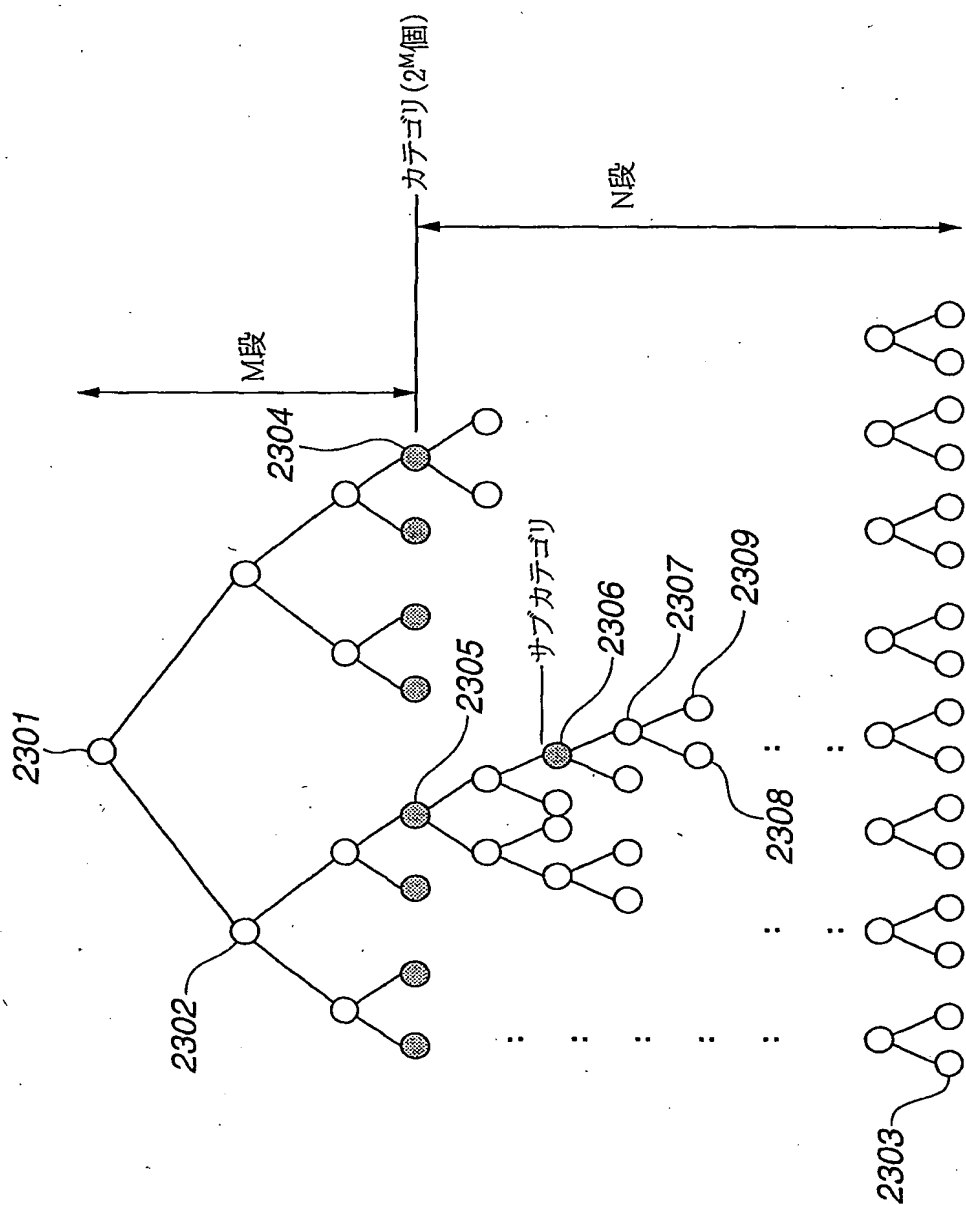


FIG.23

24/45

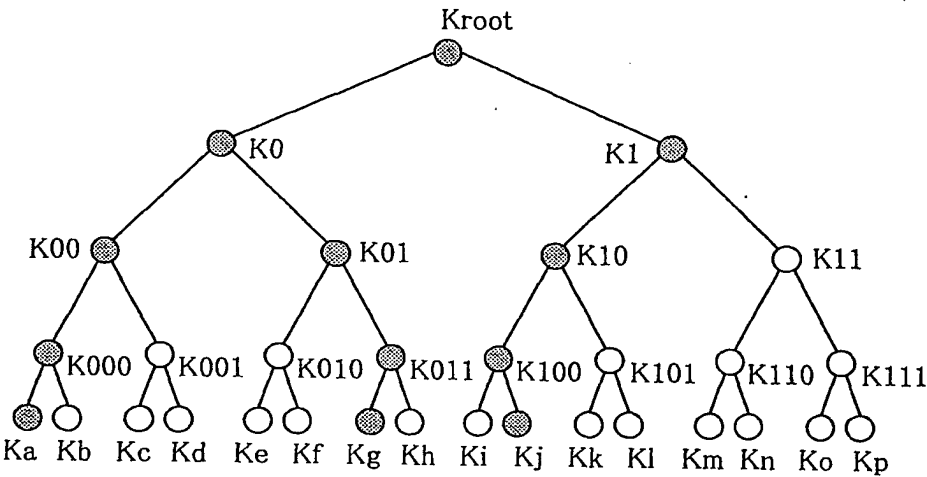


FIG.24A

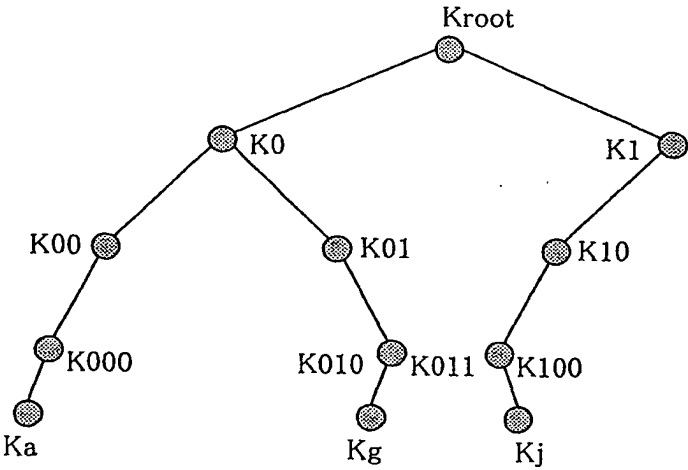


FIG.24B

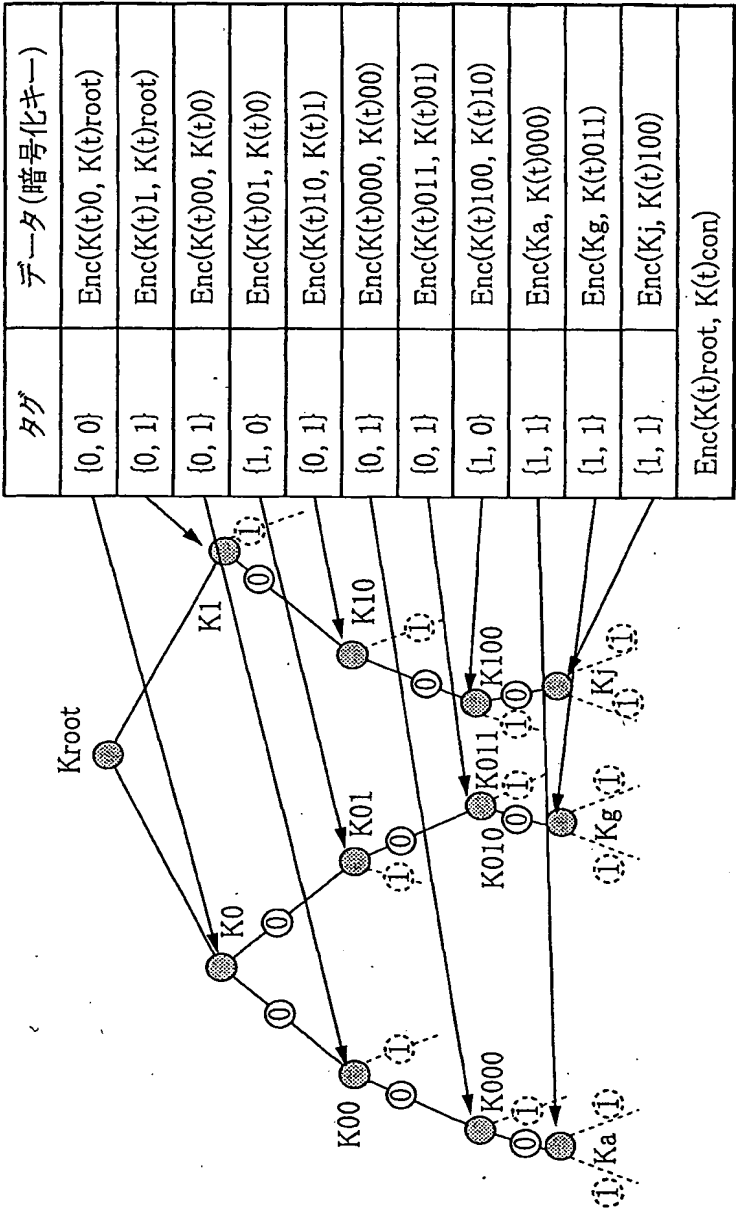


FIG.25B

FIG.25A

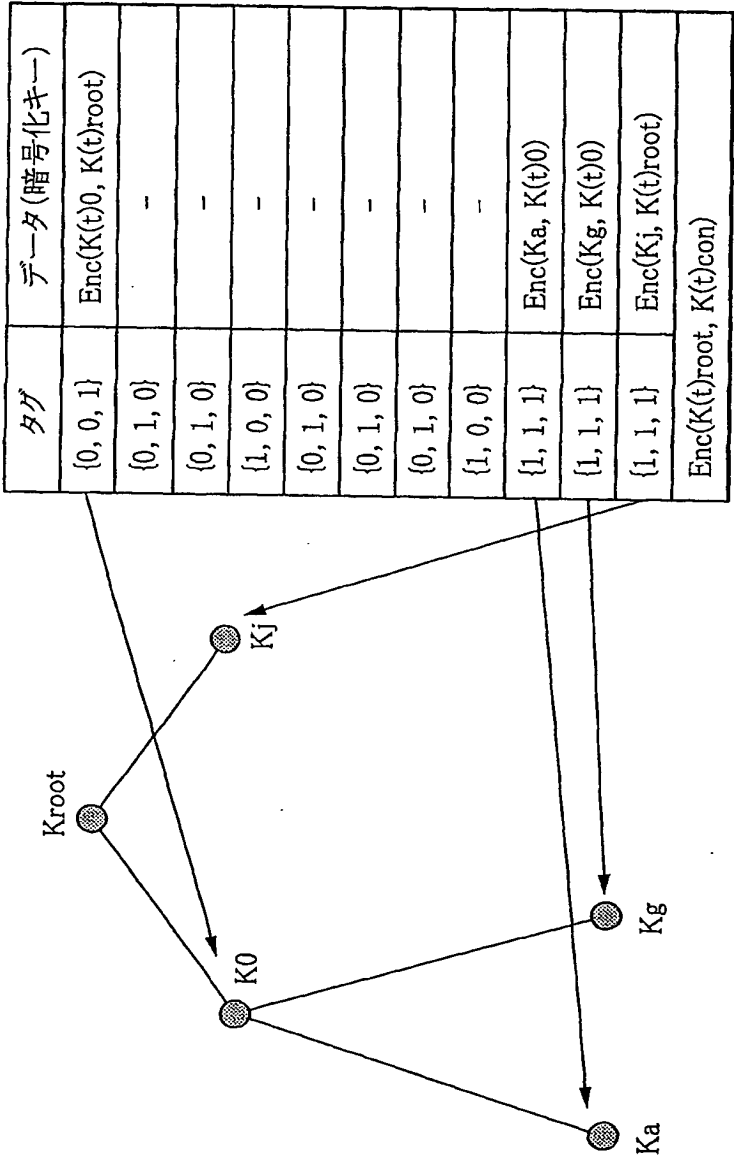


FIG.26A

FIG.26B

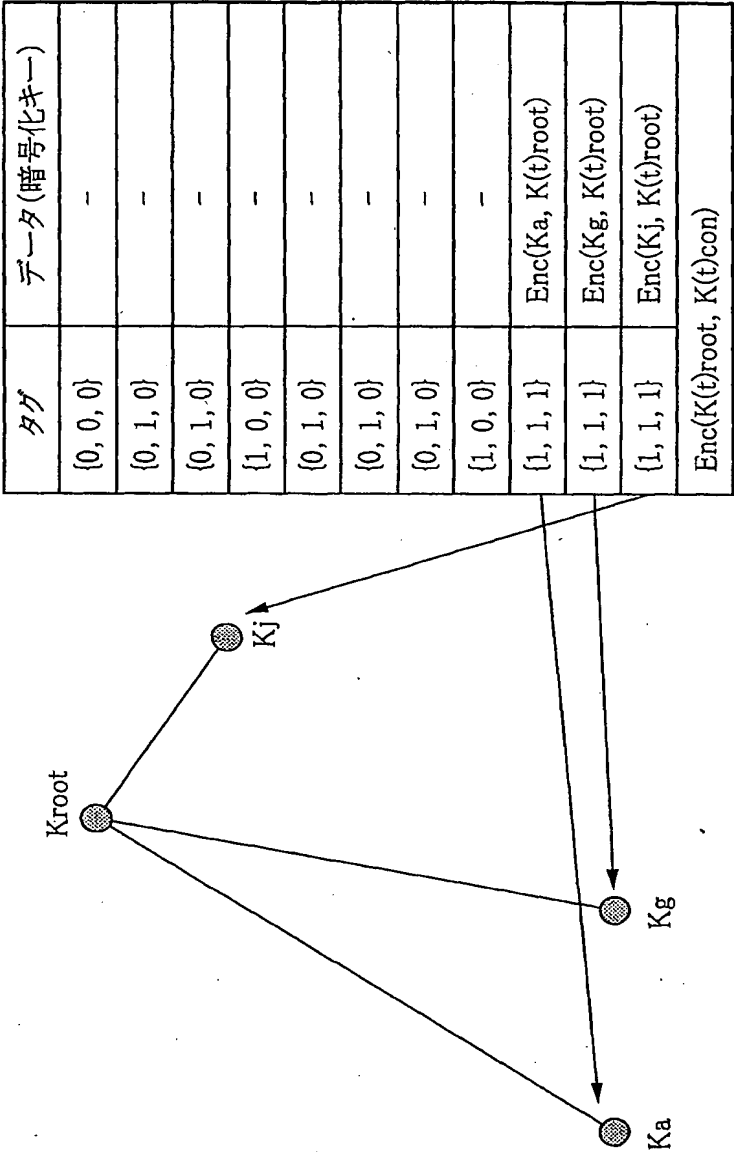


FIG.27A

FIG.27B

28/45

FIG.28A

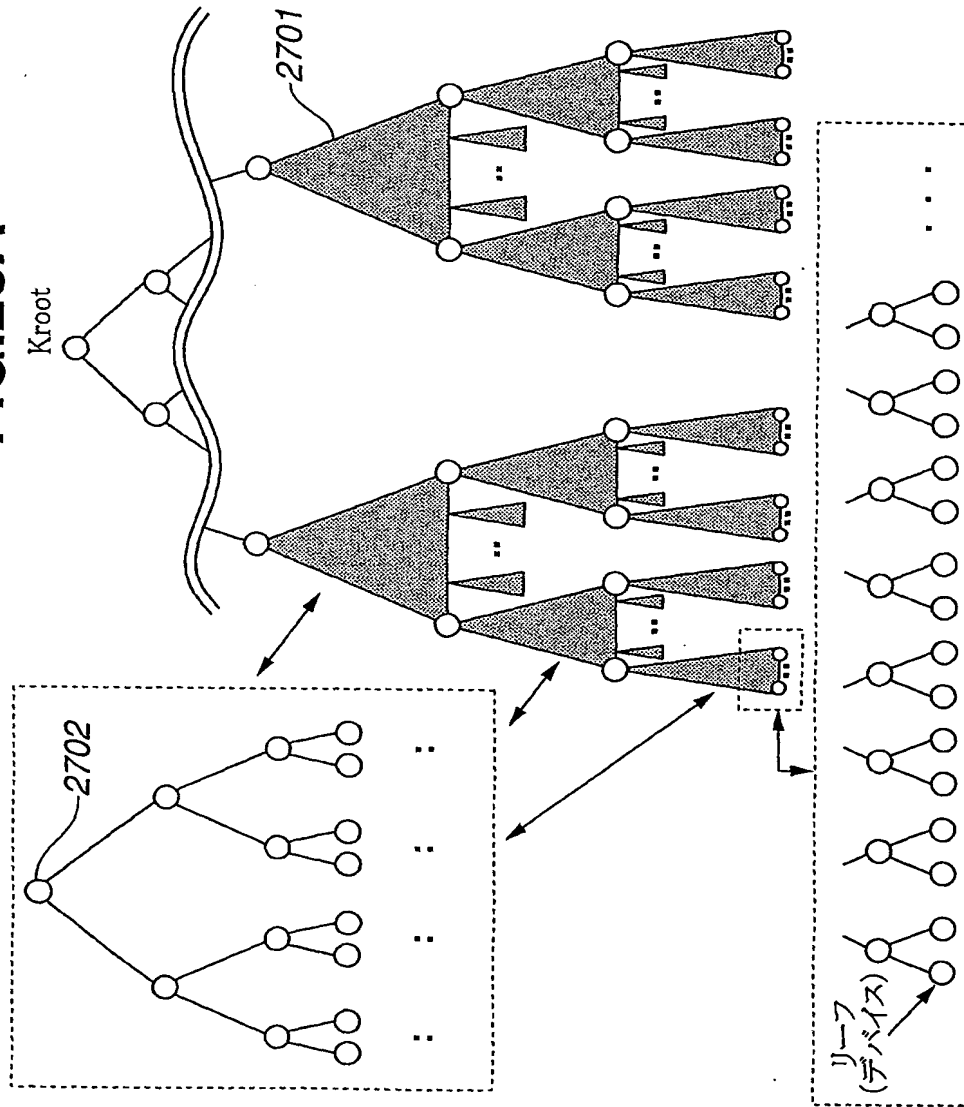


FIG.28B

FIG.28C

FIG. 29A

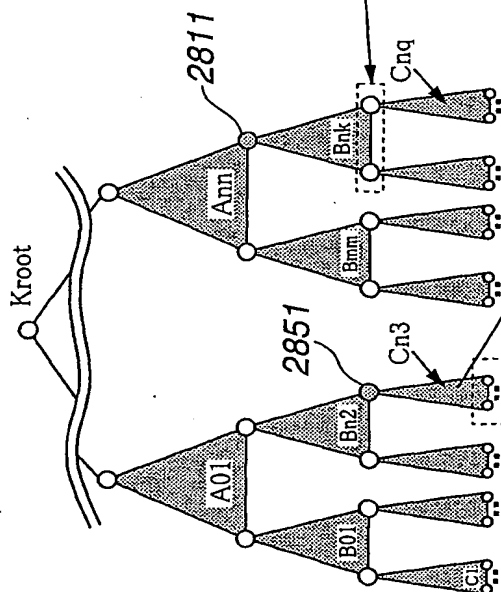


FIG. 29B

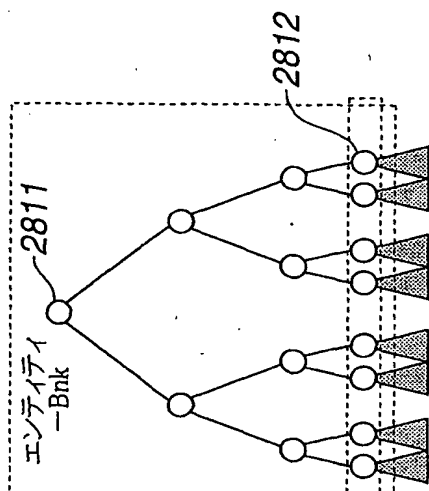
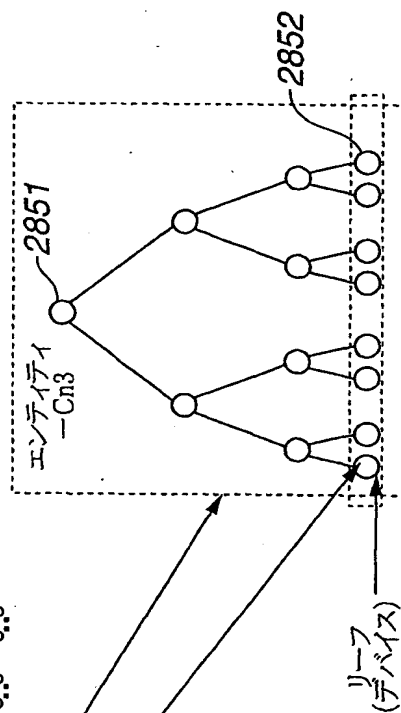


FIG. 29C



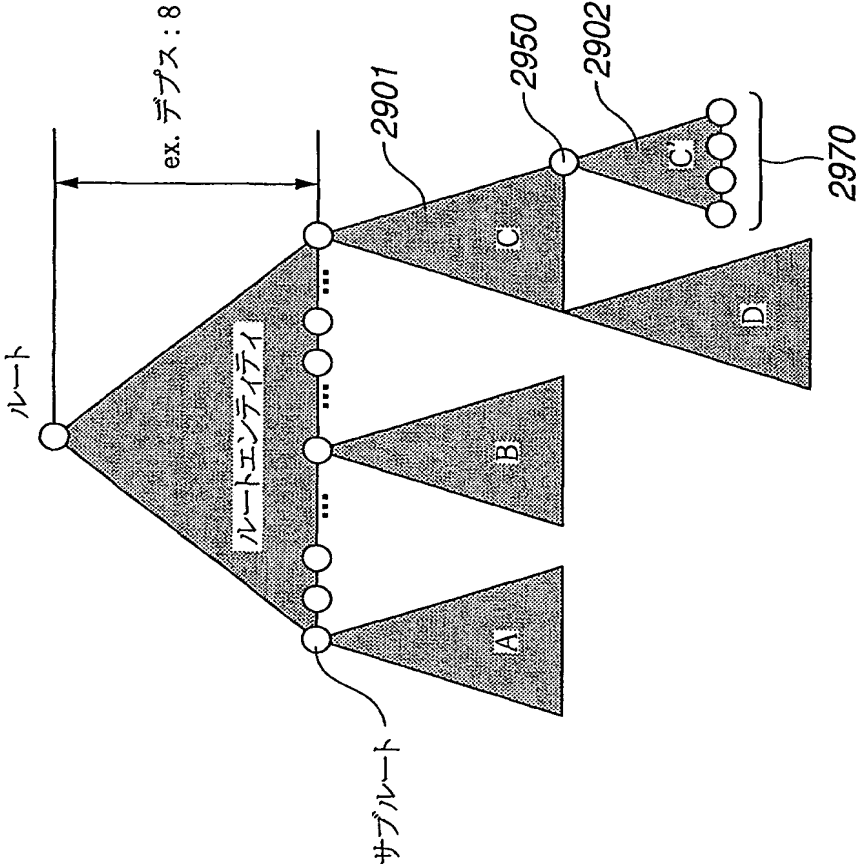


FIG.30B

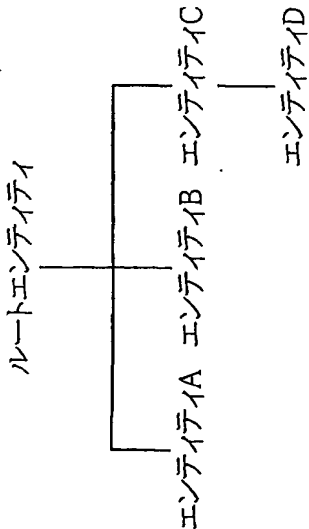


FIG.30A

31/45

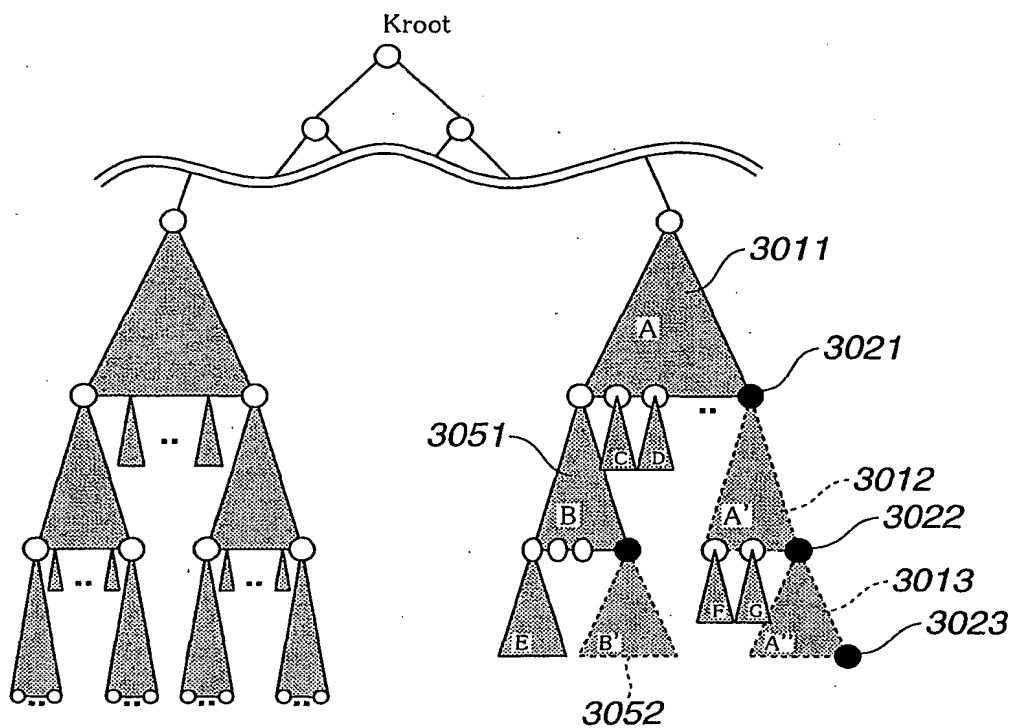


FIG.31

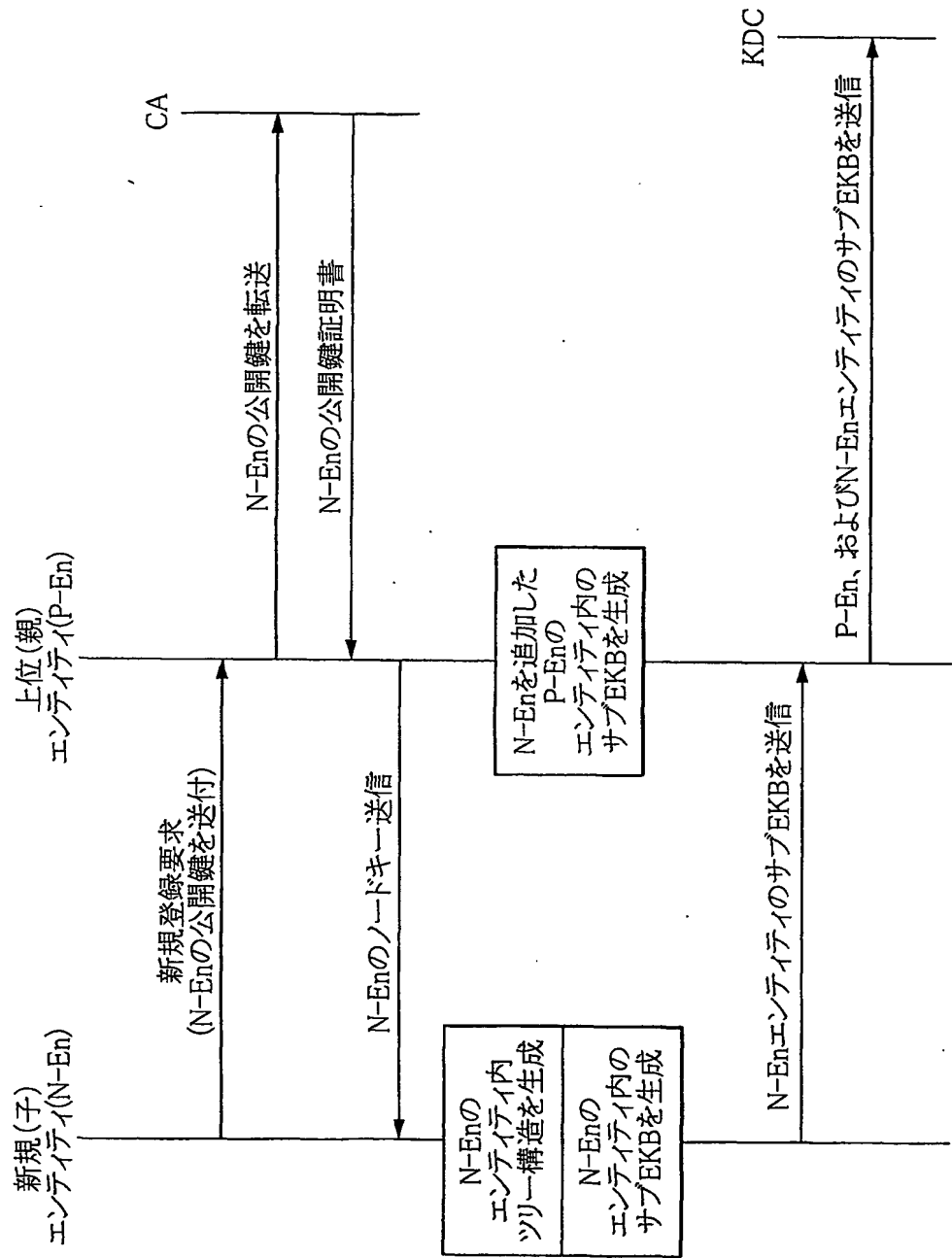


FIG.32

33/45

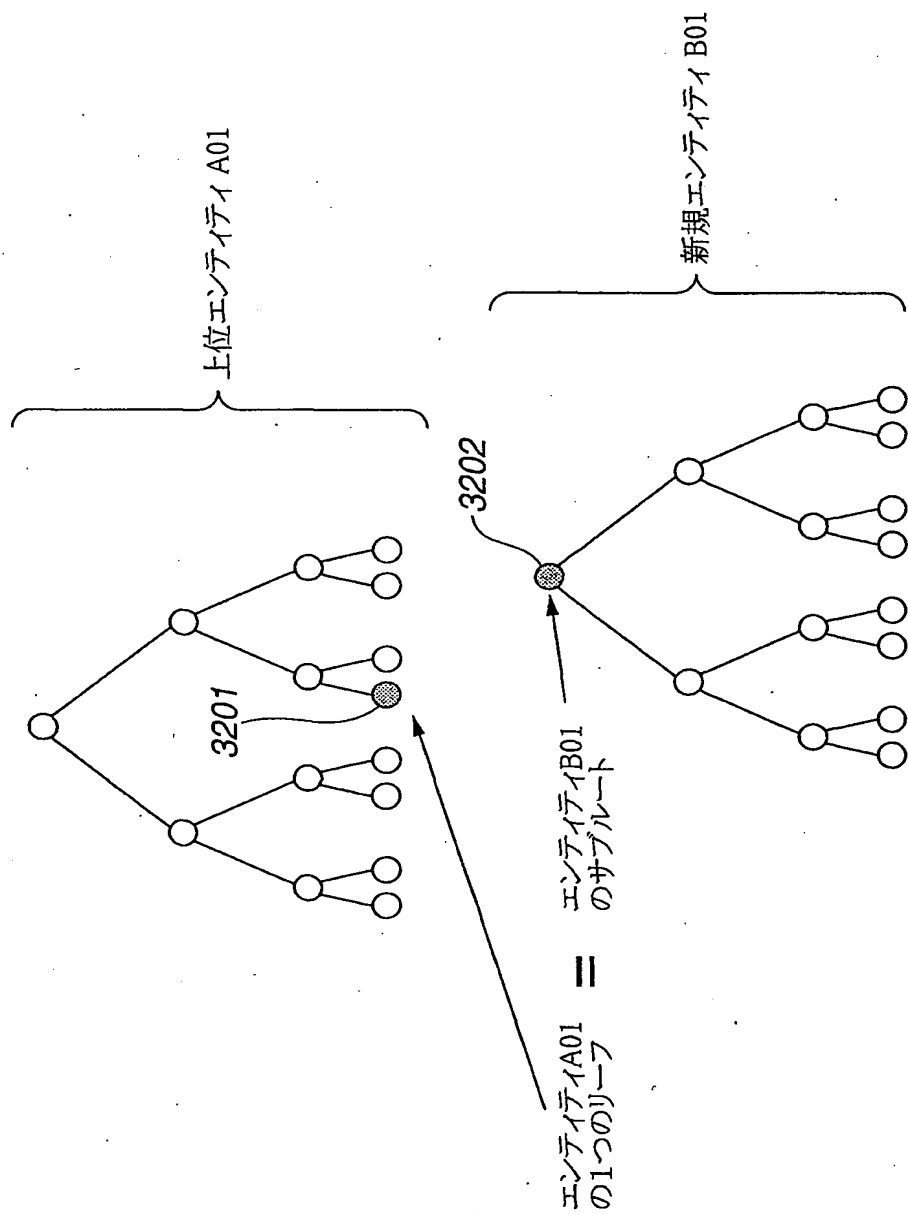


FIG.33

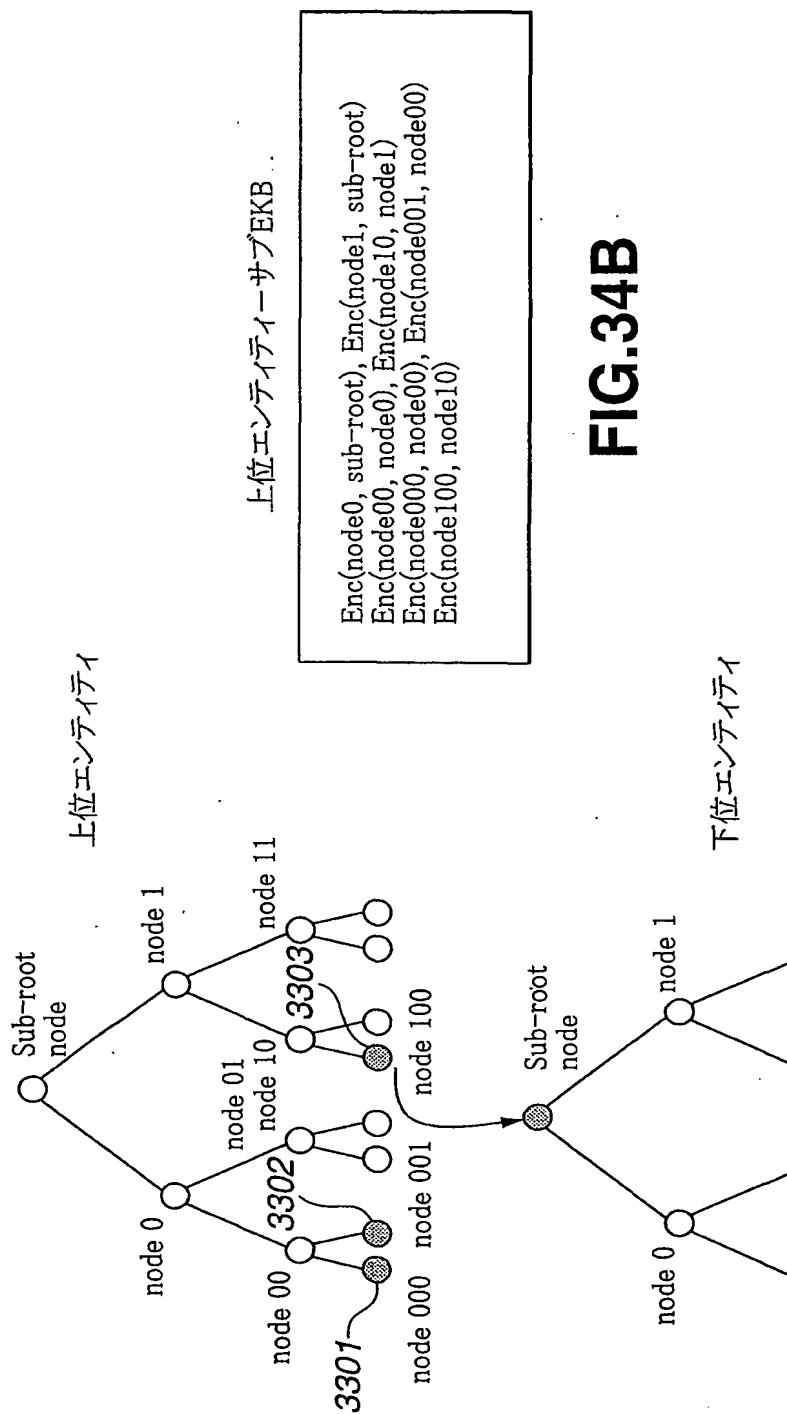
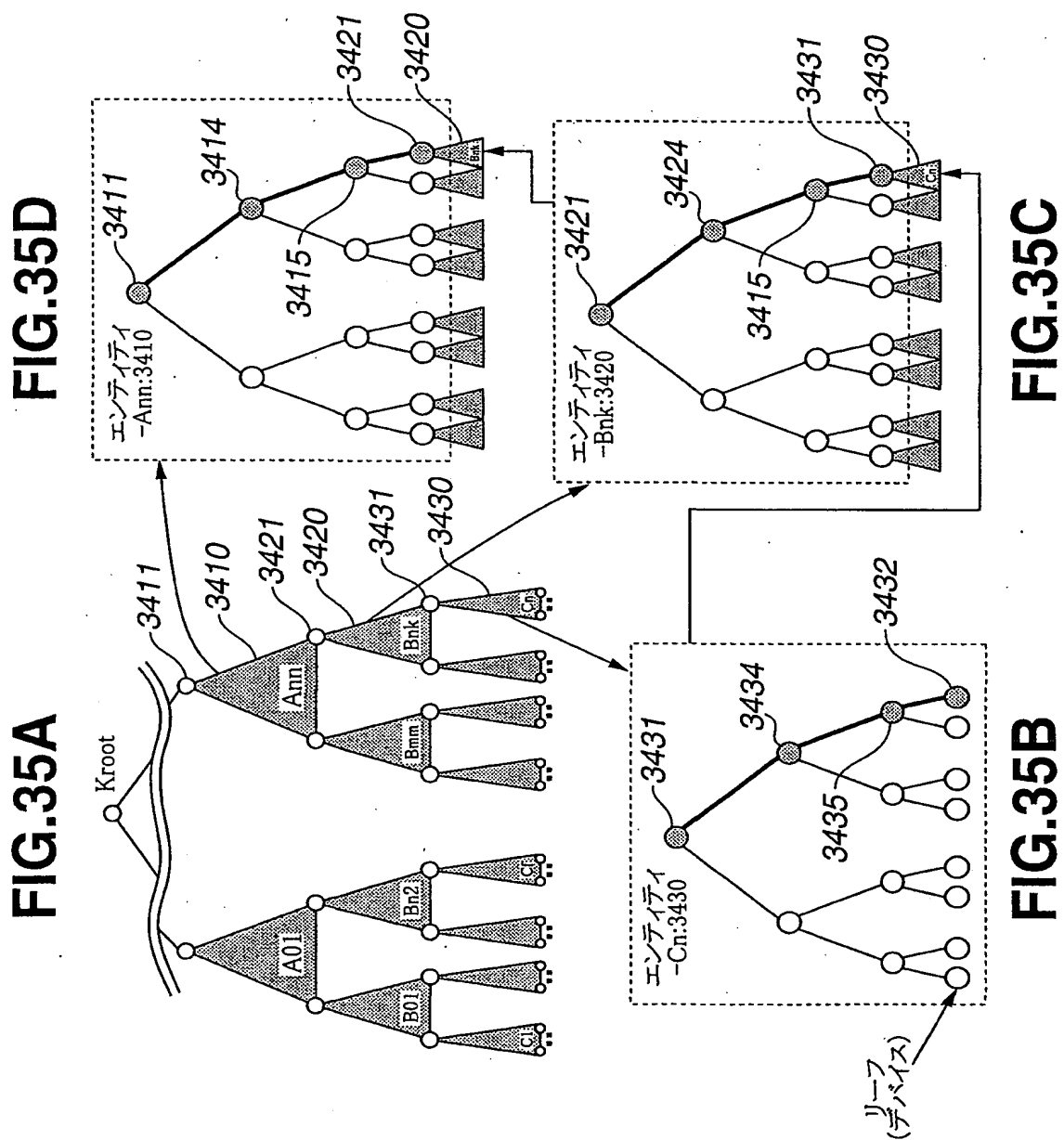


FIG. 34B

FIG. 34A



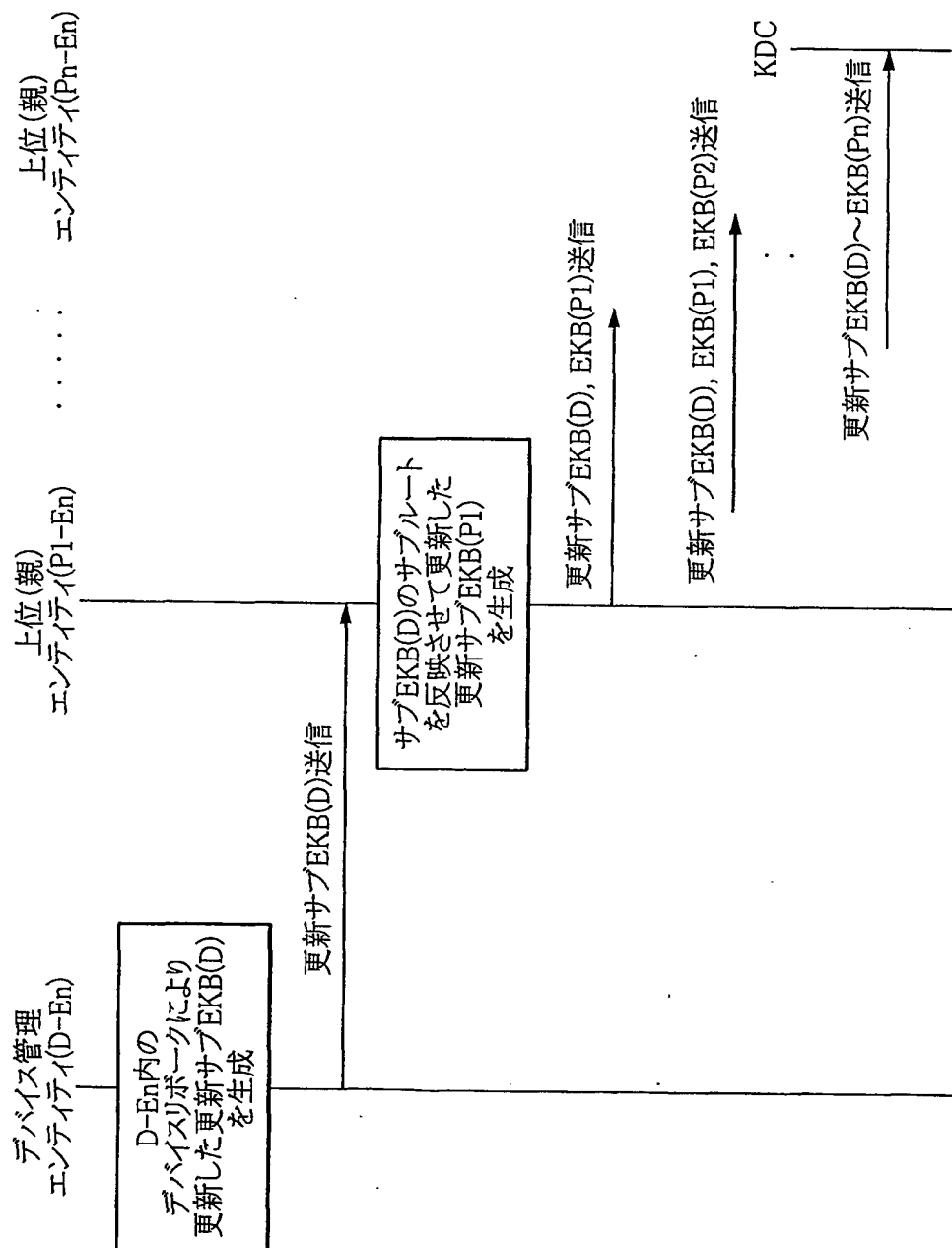


FIG.36

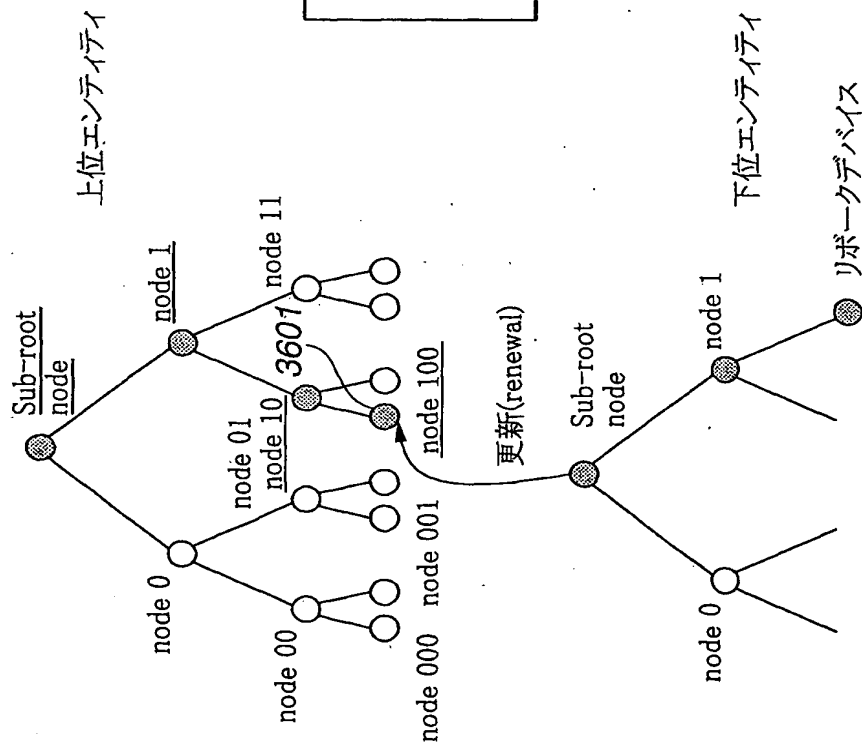
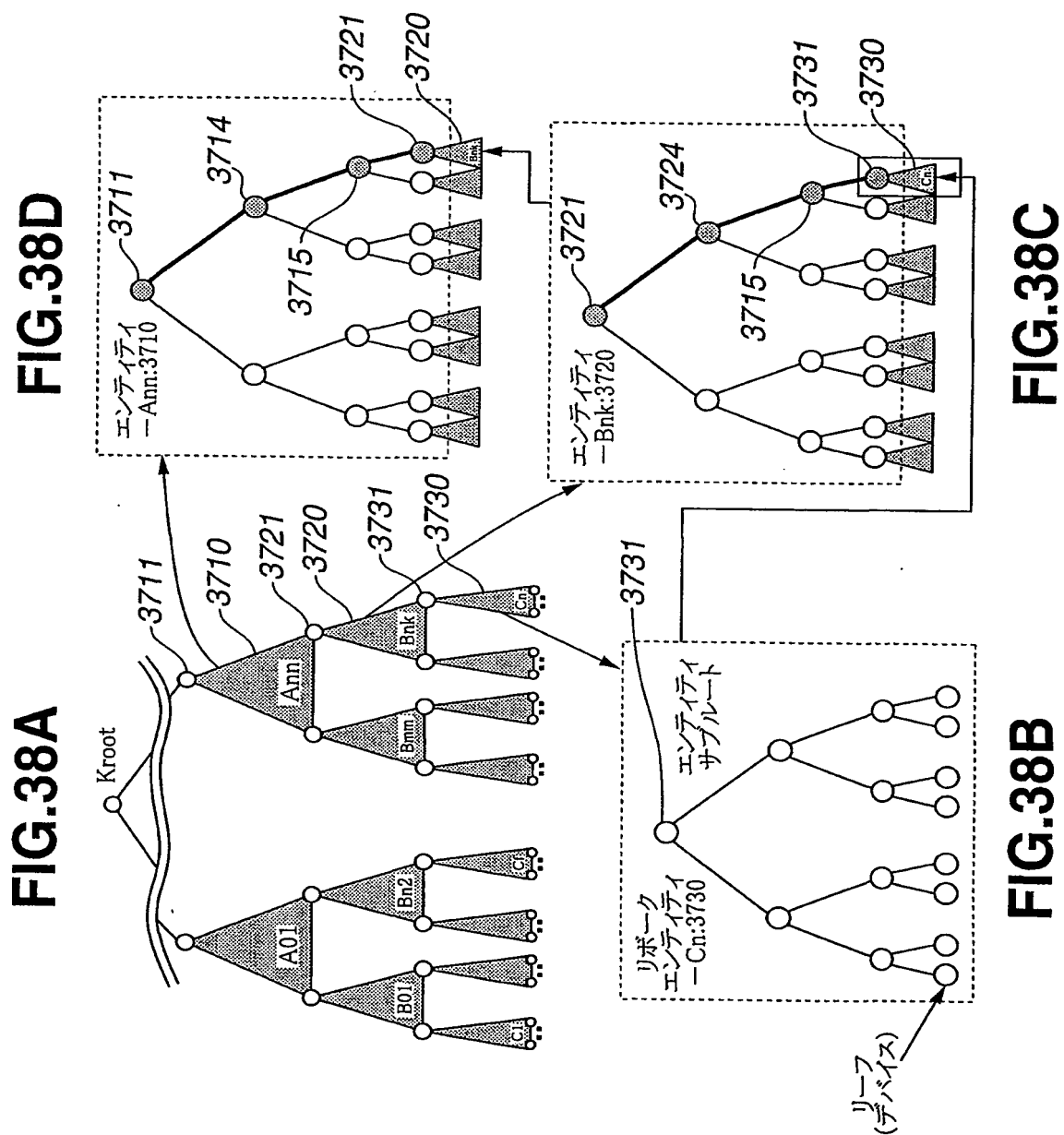


FIG.37A

上位エンティティ更新サブEKB

Enc(node0, sub-root'), Enc(node1', sub-root')
 Enc(node00, node0), Enc(node10', node1')
 Enc(node000, node00), Enc(node001, node00)
 Enc(node100', node10')

FIG.37B



39/45

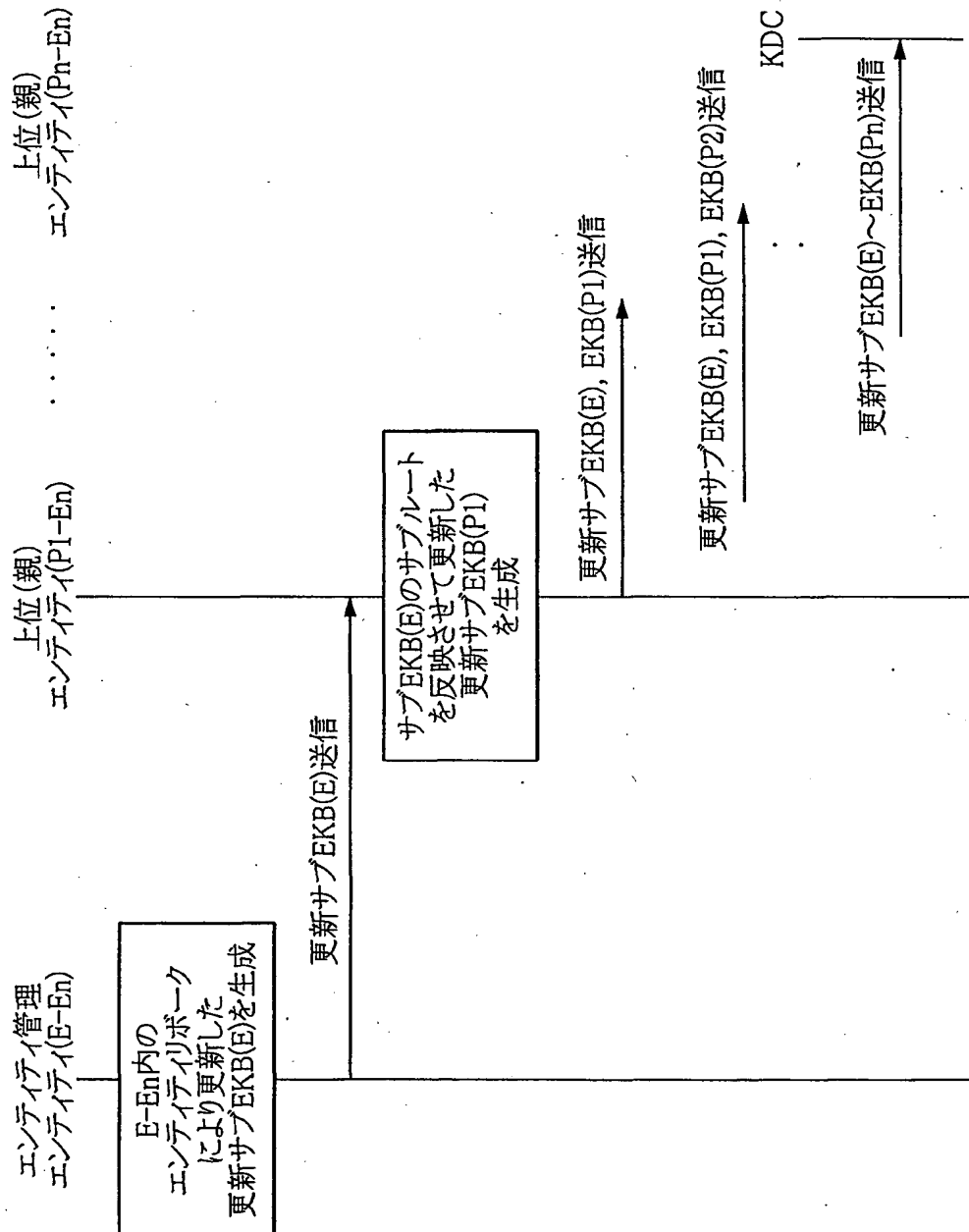


FIG.39

40/45

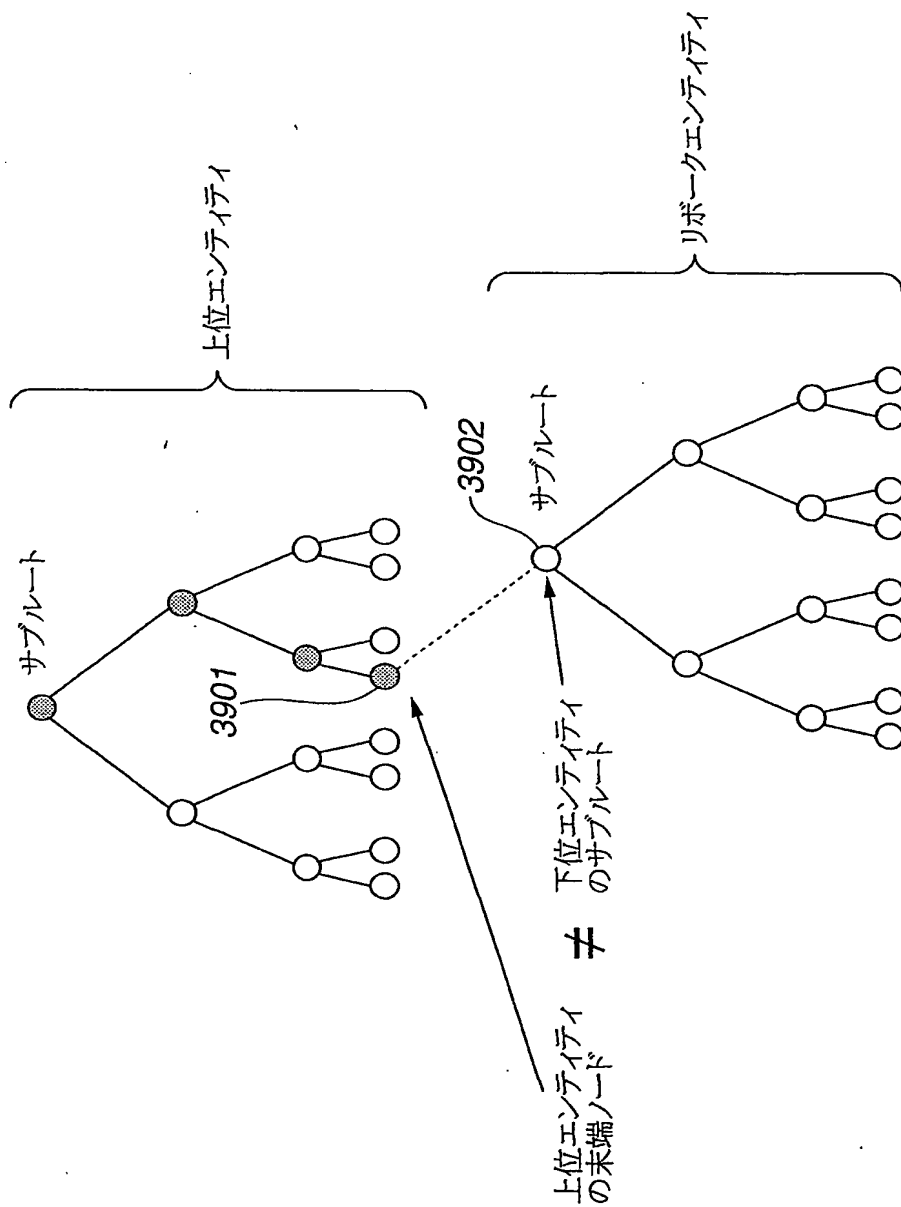


FIG.40

41/45

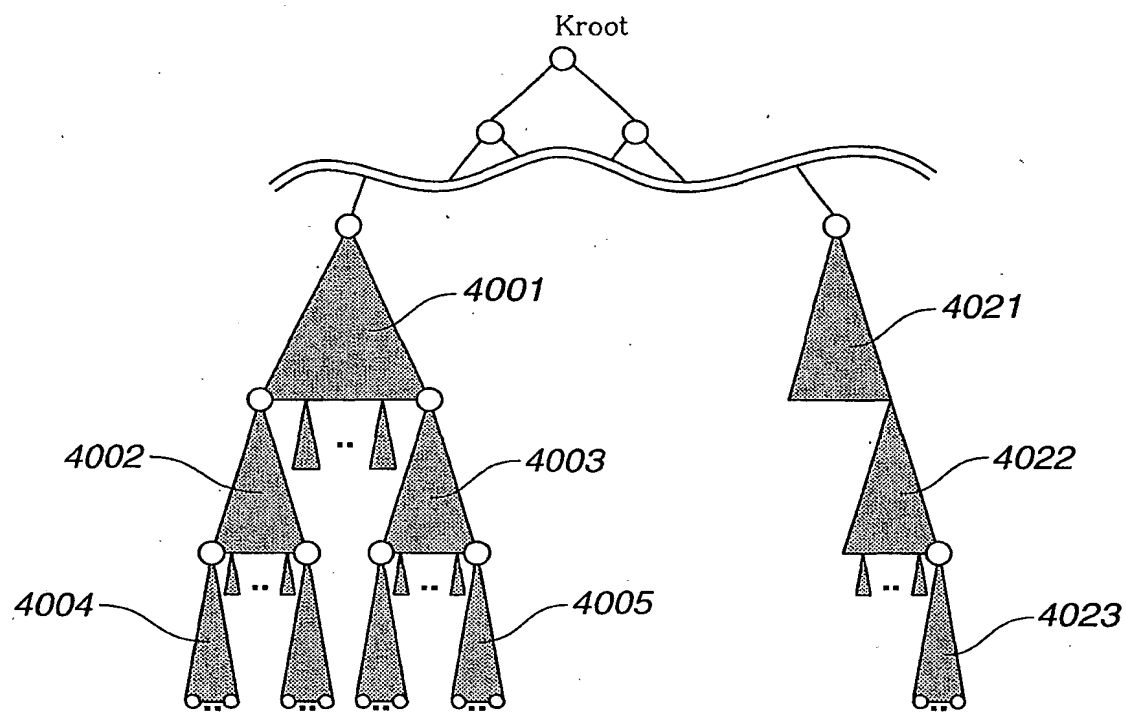


FIG.41

42/45

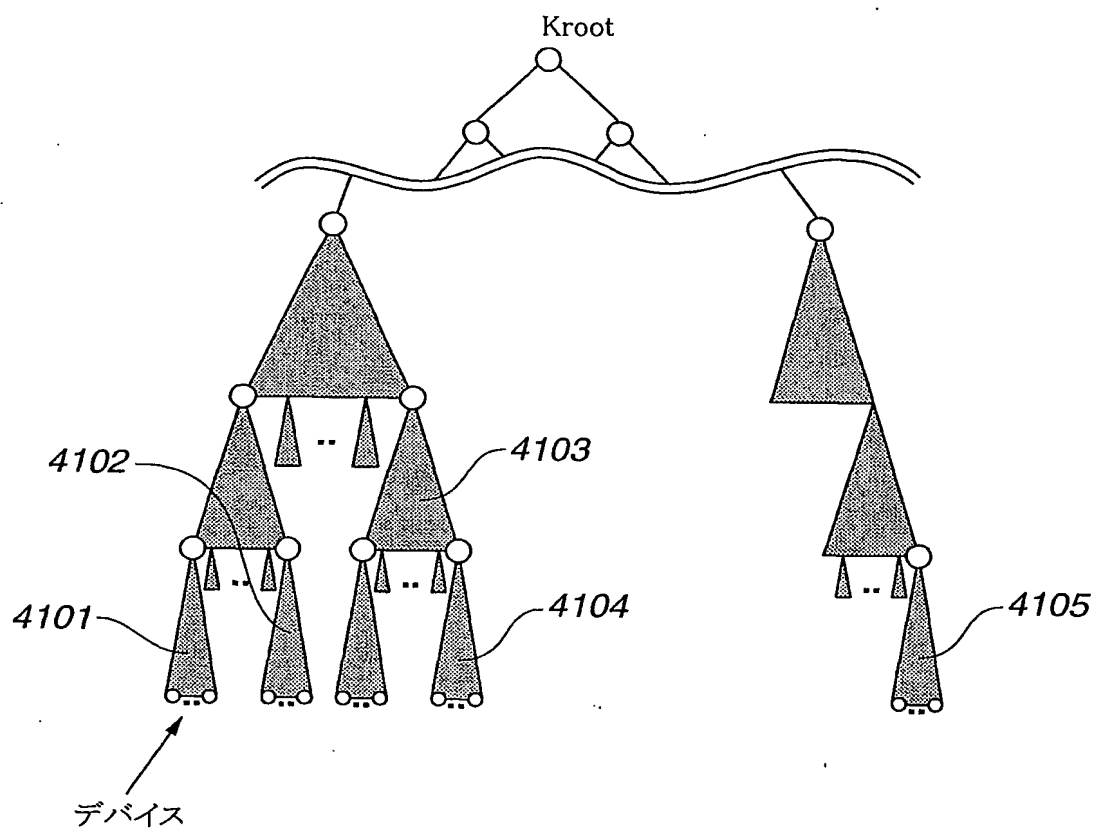
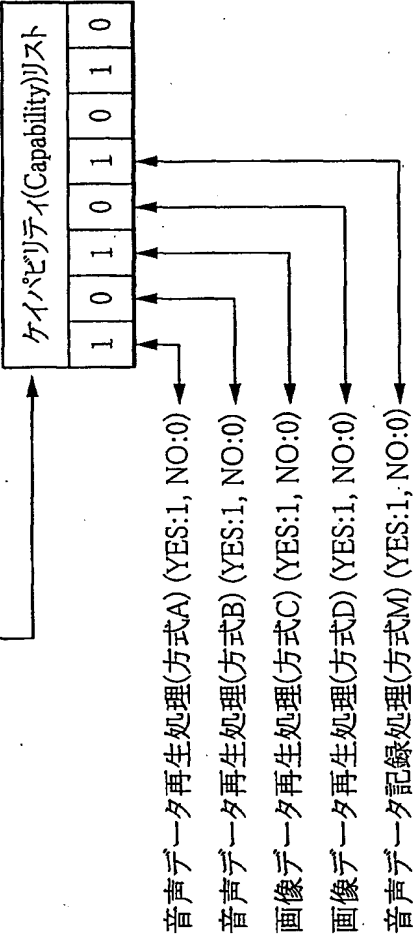


FIG.43A

ケイパビリティ(Capability)リスト										エンティティID	EKB	サブルート
1	0	1	0	1	0	1	0	1	0	Ent0010	EKB0010	K0010
0	0	1	0	0	0	1	0	1	0	Ent0011	EKB0110	K0110
1	1	1	1	1	0	0	0	0	0	Ent0012	EKB0011	K0011
:	:	:	:	:	:	:	:	:	:	:	:	:
0	0	1	1	1	0	1	1	0	1	Ent00nn	EKB00nn	K00nn

FIG.43B



44/45

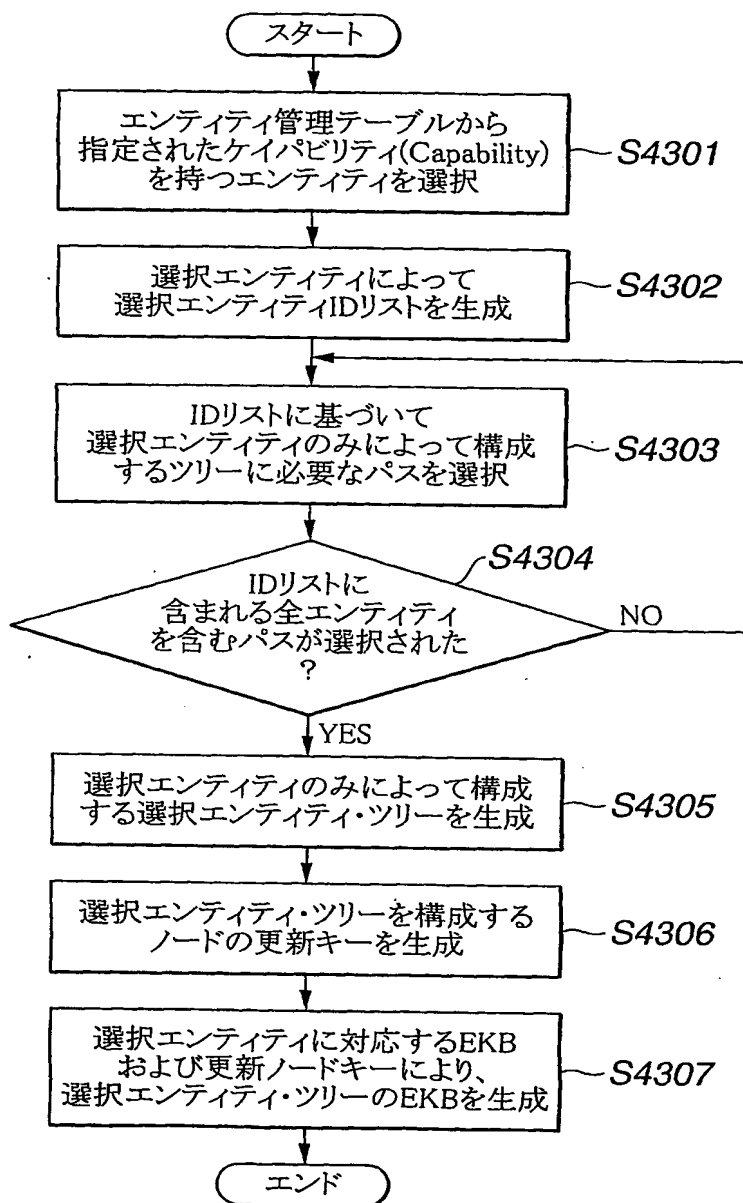


FIG.44

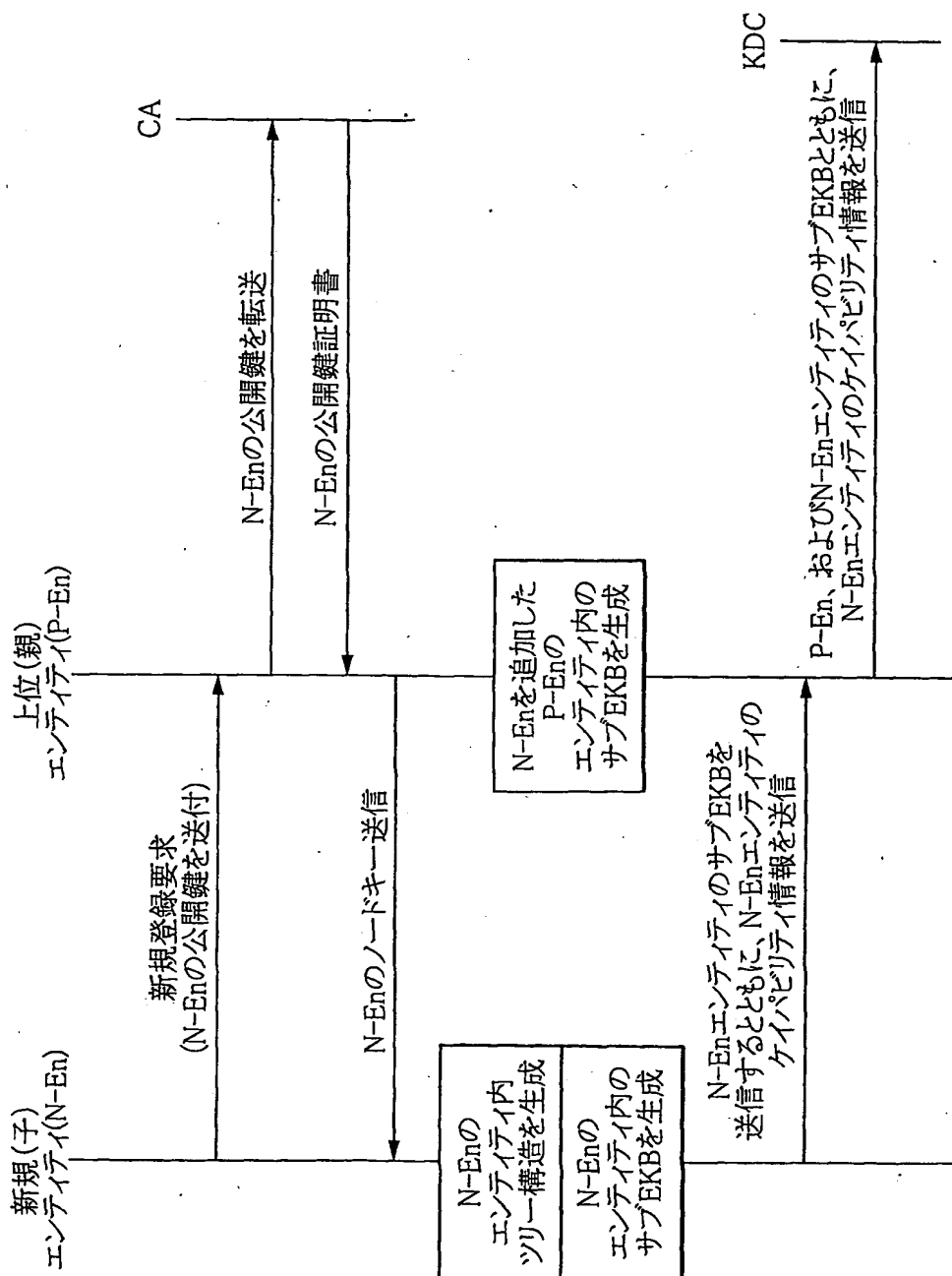


FIG.45

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02929

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST DATABASE ON SCIENCE AND TECHNOLOGY key, tree

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 11-187013, A (IBM Japan, Ltd.), 09 July, 1999 (09.07.99), Par. Nos. 9 to 11, 17 to 22	1, 8-14, 20-25, 28, 29, 33-39
A	& CN, 1224962, A	2-7, 15-19, 26, 27, 30-32
X	"The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 9, pp. 1614-1631	1, 8-14, 20-24, 28, 29, 33-39
A	September, 1999 (09.99), page 1616, right column to page 1621, left column	2-7, 15-19, 25-27, 30-32
X	"Secure Group Communications Using Key Graphs", Proceedings of ACM SIGCOMM'98, pp. 68-79	1, 8-14, 20-24, 28, 29, 33-39
A	02 September, 1998 (02.09.98), 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	2-7, 15-19, 25-27, 30-32
X	"Key management for secure Internet Multicast using Boolean Function Minimization Techniques", Proceedings of Infocom'99, Vol. 2, p. 689-698	1, 8-14, 20-24, 28, 29, 33-39

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
16 May, 2001 (16.05.01)

Date of mailing of the international search report
22 May, 2001 (22.05.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02929

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	24 March, 1999 (24.03.99) II. KEY MANAGEMENT SCHEME (http://www.ieee-infocom.org/1999/)	2-7, 15-19, 25-27, 30-32
EX	US, 6049878, A (Sun Microsystems, Inc.), 11 April, 2000 (11.04.00), Full text (Family: none)	1, 8-14, 20-24, 28, 29, 33-39
A	US, 5748736, A (S, Mittra), 05 May, 1998 (05.05.98), Full text (Family: none)	1-39
EA	WO, 01/03364, A1 (Matsushita Electric Ind. Co., LTD.), 11 January, 2001 (11.01.01), Full text (Family: none)	1-39
EA	WO, 01/03365, A1 (Matsushita Electric Ind. Co., LTD.), 11 January, 2001 (11.01.01), Full text (Family: none)	1-39

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
WPI, JICST科学技術文献データベース key, tree		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 11-187013, A (日本アイ・ビー・エム株式会社) 9. 7月. 1999 (09. 07. 99) 第9-11, 17-22段落 & CN, 1224962, A	1, 8-14, 20- 25, 28, 29, 33- 39
A		2- 7, 15-19, 26, 27, 30-32
X	"The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 9, p. 1614-1631. 9月. 1999 (09. 99) 第1616頁右欄-第1621頁左欄	1, 8-14, 20- 24, 28, 29, 33- 39
A		2- 7, 15-19,
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	16. 05. 01	国際調査報告の発送日
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 中里 裕正
		5M 9364 電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
		25-27, 30-32
X	"Secure Group Communications Using Key Graphs", Proceedings of ACM SIGCOMM'98, p.68-79 2. 9月.1998(02.09.98) 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1, 8-14, 20- 24, 28, 29, 33- 39
A		2- 7, 15-19, 25-27, 30-32
X	"Key management for secure Internet Multicast using Boolean Function Minimization Techniques", Proceedings of Infocom'99, Vol.2, p.689-698 24, 3月.1999(24.03.99) II. KEY MANAGEMENT SCHEME (http://www.ieee-infocom.org/1999/)	1, 8-14, 20- 24, 28, 29, 33- 39
A		2- 7, 15-19, 25-27, 30-32
EX	US, 6049878, A (Sun Microsystems, Inc.) 11, 4月.2000(11.04.00) 全頁を参照(ファミリー無し)	1, 8-14, 20- 24, 28, 29, 33- 39
A	US, 5748736, A (S. Mittra) 5, 5月.1998(05.05.98) 全頁を参照(ファミリー無し)	1-39
EA	WO, 01/03364, A1 (Matsushita Electric Industrial Co., LTD.) 11. 1月.2001(11.01.01) 全頁を参照(ファミリー無し)	1-39
EA	WO, 01/03365, A1 (Matsushita Electric Industrial Co., LTD.) 11. 1月.2001(11.01.01) 全頁を参照(ファミリー無し)	1-39

THIS PAGE BLANK (USPTO)